

PRIVACY TOWARDS 2020

EXPERT VIEWS

Focus on key transformations at the crossroads between usage, technology and economic strategies

What is the new landscape for personal data, freedoms and privacy?

Protecting, regulating and innovating in the future



The collection of IP (Innovation & Prospective) Reports, is intended to present and share the future studies carried out by the CNIL DEIP (Department for Studies, Innovation and Foresight) and by its innovation lab. The aim is therefore to help foster debate and give “food-for-thought” in the field of IT and Freedoms.



Commission Nationale de l'Informatique et des Libertés
Direction des études, de l'innovation et de la prospective
8 rue Vivienne – CS 30223 – 75083 Paris Cedex 02
Tel.: +33 (0)1 53 73 22 32 – Fax: +33 (0)1 53 73 22 00 – deip@cnil.fr
Biannual Publication
Publishing Director: Édouard Geffray
Editor-in-Chief: Sophie Vulliet-Tavernier
Graphic Design: EFIL +33 (0)2 47 47 03 20 / www.efil.fr
Printing: ImprimPlus (Essonne)
Photo credits: Fotolia, istockphoto, @identitywoman
ISSN: pending
Legal deposit: on publication

The points of view expressed in this publication do not necessarily reflect the position of the CNIL.

Follow the CNIL on...



COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

IP REPORTS

INNOVATION & FORESIGHT

NO. 01

The editing of this report and supervision of its design and printing was undertaken by the CNIL DEIP (Olivier Coutor, Geoffrey Delcroix, Olivier Desbiey, Marie Leroux, and Sophie Vulliet-Tavernier, with the assistance of Caroline Chemouilli and Nicolas Carougeau).

EDITORI

Part 0.1

Focus on key transformations in the cross-over between usage, technology and economic strategy

THE SOCIAL INTERNET REVOLUTION: WILL WE ALL BE "CELEBRITIES" IN THE FUTURE?	12
DATA AT THE HEART OF BUSINESS MODELS: WILL WE ALL BE DATA TRADERS IN THE FUTURE?	15
THE ALGORITHM "DICTATORSHIP": WILL WE ALL BE CALCULATED IN THE FUTURE?	18
GEOLOCATION: WHERE ARE WE HEADED?	21
BIOMETRICS: THE NEW "OPEN SESAME"?	24
NANOTECHNOLOGY, GENETICS, NEUROSCIENCE, "ENHANCED HUMANS": WHAT IS ENVISIONED FOR HUMANITY IN THE FUTURE?	28

Part 0.2

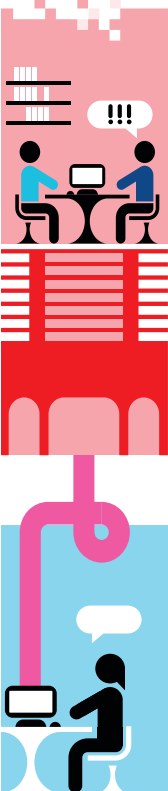
What is the new landscape for personal data, freedoms and privacy?

IS EVERYTHING BECOMING PERSONALLY IDENTIFIABLE INFORMATION?	32
MORE AND MORE NEW SENSITIVE DATA?	34
PRIVACY PARADOX: A MYTH OF BENIGN NEGLECT ?	36
DIGITAL IDENTITY/IES: AUTHENTICATION FOR ALL?	38
ARE WE HEADED FOR NEW DIGITAL DIVIDES?	40

Part 0.3

Protecting, regulating and innovating for tomorrow

DEFENCE OF PRIVACY OR FREEDOMS?	44
PROTECT WHOM, PROTECT WHAT AND HOW?	46
INNOVATIONS IN REGULATION	50
RETHINKING DIGITAL LAW ?	54



AL

What will be the key issues for personal data protection towards 2020? What will your privacy look like? What will become of our digital freedoms in the "everyone and always connected" age? And what forms will regulation need to take in order to meet these new challenges? These are the key questions that we put to over forty experts across a range of fields between autumn 2011 and spring 2012. Indeed, with the explosion of personal data *via Big Data*, and the proliferation of new uses that consume ever more information, a regulator cannot and should not act alone. It has to listen, exchange and assemble communities of opinions and ideas so as to be able to understand the complex environment within which it operates.


The objective of this first edition of the Innovation & Foresight Report, a new CNIL publication, is to bring together these expert opinions. These experts have shared with us their visions – which naturally sometimes differ – of the key transformations and future developments in the field of privacy, freedoms and personal data, and their assessments – all highly instructive – of future forms of regulation. We shall be presenting and endeavouring to understand these visions and assessments, in order to see what use can be made of them by the regulator.

This initiative reflects a new impetus that I would like the CNIL to espouse. There is now a need for the CNIL to develop a network culture and to work increasingly with regulation "stakeholders". Our Commission must be able to evolve and to adjust its methods of intervention if it is to remain relevant. It must develop its analysis in the area of forecasting to better understand technological developments and new uses, and to anticipate and assess the new key issues for data protection. It must be confirmed as a pragmatic and credible regulator that is capable of proposing operational solutions. It must therefore invest, as far as its means permit, in research conducted in these fields, and in piloting and commissioning work that it considers to be of particular importance.

In 2011, we established a Department for Foresight. The "Foresight Committee", created in May 2012, constituted a second, outward-looking stage, drawing upon a range of talent and public figures.

The launch of the IP Reports and the organisation of a day of debate around its content constitute another stage in the process. These Reports and the debate surrounding their content will allow our institution to build up a research community (researchers, *think tanks*, developers and sector experts, both French and international) on the issues of personal data protection. The CNIL has a need for this community in a wide range of areas to discover new solutions and for periodic self-examination.

Our society is undergoing profound change under the combined impacts of technological developments, emerging business models and constantly evolving digital business practices. With a new legal framework being developed at the European level, the issue of personal data protection is, more than ever, at the centre of the debate. It concerns all stakeholders – citizens, governments, major players in the digital world, other companies, public services – and has reached a crossroads where multiple paths intersect – economic, social, legal – at both the national and the international levels.

I feel that innovation is emerging from the exchange of views and the pooling of ideas and resources, including in the field of regulation, so that, collectively, the ethical framework of the future digital world may be established. 

Isabelle Falque-Pierrotin,
CNIL President

42 EXPERTS

ASSISTING THE CNIL

This first edition of the IP Reports is devoted to the resumption of a foresight project that began in 2011 and led by the CNIL Department for Studies, Innovation and Foresight (DEIP), on the subject of: "Privacy, freedoms and personal data towards 2020. What are CNIL's priorities for protection and regulation? Positions, perceptions and expectations of stakeholders."

This project involved, between September 2011 and April 2012, over forty interviews with experts across a wide range of fields: sociologists, economists, philosophers, jurists, historians, communication sciences and IT security researchers, and representatives of companies and associations in digital and rights protection fields.

The objective was to:

- compare these outward manifestations with the perceptions of the CNIL (for example through debates, events and study days such as the "Privacy 2020" study day);
- confronter ces représentations externes aux perceptions de la CNIL (par exemple au travers de débats, événements et journées d'études comme la journée « vie privée 2020 »);
- incorporate experts into the forecasting work and reflections of the CNIL in a spirit of constructive dialogue.

To this end, an interview form (see page 58 "appendix"), was compiled using open questions, taking into account the following aspects:

- perception of major developments (technological, economic, societal, etc.) in the sphere of privacy, freedoms and personal data: trends, uncertainties and possible breaches;

- current and future transformations in the relationship between individuals and society and privacy and personal data;
- how experts envision future forms of regulation, and how they anticipate and interpret the role of data protection authorities in the future;
- and in relation to stakeholders, their plans, and their directions within the field in question.

These interviews enabled a dossier to be compiled, which is the principal subject of this report. The "Privacy towards 2020" one-day workshop, organised on 30 November 2012, was an extension of this.

Of course, this IP Report was not intended to be a definitive or exhaustive document on the vast subject of "Privacy towards 2020" or to expound the CNIL doctrine. Rather it aims to provide a dynamic panorama of the contrasting visions of the key transformations at work.

Like the "Privacy towards 2020" workshop, this report will, we hope, provide a starting point for areas of research to be explored jointly and for concerted forward-looking thinking.

ACKNOWLEDGEMENTS

Once again, we would very much like to thank all of the experts for their unfailingly detailed and fascinating contributions, and for taking the time to meet with us, to answer our long list of questions, and finally to provide their views on the content of this report.

All of the DEIP team extend their heart-felt thanks to Nathalie Bassaler and François Bourse, foresight consultants at Magellis Consultants and GERPA, for their vital coaching and advice, in the undertaking of this initial work package.

LIST OF THE 42 EXPERTS

Maryse Artiguelong Deputy Secretary General of the Human Rights League (LDH)

Christine Balagué Holder of Social Networks Chair at the Institut Mines-Telecom. Joint-President of the Renaissance Numérique think tank

Arnaud Belleil Deputy Managing Director of Security.com. Honorary Vice-President of the French Association of Correspondents for Personal Data Protection (AFCDP)

Pierre-Jean Benghozi CNRS Research Director and Professor at the École Polytechnique, Head of the Economics and Management Research Unit and Holder of the Chair in "Innovation and Regulation of Digital Services". Member of the CNIL "Foresight Committee"

Alain Bensoussan Barrister at the Paris Court of Appeal. Lecturer for IT Law at the École Centrale de Paris

Dominique Boullier University Professor. Sociology Lecturer at Sciences Po Paris. Scientific Coordinator of the Medialab of Science Po Paris

Stefana Broadbent Psychologist and Professor in Digital Anthropology at University College London (UCL). Head of Master's in Digital Anthropology at UCL Anthropology Department. Member of the CNIL "Foresight Committee"

Dominique Cardon Sociologist at Orange Labs' SENSE Usage Think-Tank. Associate Researcher at the Centre for the Study of Social Movements of the École des Hautes Études en Sciences Sociales (CEMS/EHESS). Member of the CNIL "Foresight Committee"

Antonio Casilli Sociologist and Lecturer in "Digital Humanities" at Telecom ParisTech. Associate Sociology Researcher at the Centre Edgar Morin (EHESS, Paris)

Claude Castelluccia Inria Research Director. Head of Inria Privatics Team (IT and Privacy Protection)

Isabelle De Lamberterie Research Director at the Centre for Studies on International Legal Cooperation (CECOJI) of the CNRS

Mireille Delmas-Marty Law Professor and Holder of the Chair in "Comparative Legal Studies and Internationalisation of Law" at the Collège de France. Member of the Academy of Moral and Political Sciences

Dominique Desjeux Professor of Social and Cultural Anthropology at Université Paris Descartes, Faculty of Human and Social Sciences, Sorbonne

Yves Deswarte Research Director at CNRS within the LAAS (Systems Architecture and Analysis laboratory) research unit

David Forest Barrister at the Paris Court of Appeal. Doctor of Privacy Law and Doctor of Political Science. Head of Teaching of Information Technology Law at Université de Paris I, Paris VII and Paris XI

Jean Frayssinet Professor Emeritus, Law Faculty of Université Aix-Marseille III. Member of the INTERPOL File Monitoring Commission

Paul-Olivier Gibert President of Digital & Ethics. President of the French Association of Correspondents for Personal Data Protection (AFCDP)

Olivier Iteanu Advocate at the Paris Court of Appeal. Head of Teaching in Digital Law at Université Paris XI and Paris I

Francis Jauréguiberry Sociologist and Professor at Université de Pau et des Pays de l'Adour. Director of Society Environment Territory (SET) laboratory at the CNRS

Josiane Jouët Professor and Research Director in Information and Communication Sciences at Université Panthéon Assas. Doctor of Sociology

Daniel Kaplan Co-founder and Delegate-General of the Fondation Internet Nouvelle Génération (FING) think tank

Emmanuel Kessous Professor of Sociology at Université de Sophia-Antipolis. Researcher at GREDEG (UMR CNRS 7321) and Associate Researcher at GEMASS (Paris IV - UMR CNRS 8598)

Caroline Lancelot-Miltgen Teaching Professor in Management Sciences at Université d'Angers. Researcher at GRANEM (Angers Economics and Management Research Group)

Daniel Le Métayer Inria Research Director. Manager of Inria Project Lab CAPPRIIS for the Protection of Privacy. Member of the CNIL IT and Freedoms Thesis Examining Panel

Yann Leroux Doctor of Psychology. Member of the Observatory of Digital Worlds in Human Sciences

Philippe Lemoine CEO of LaSer. Chairman of FING and the Forum d'Action Modernités. Former CNIL Member and former CNIL Commissaire du Gouvernement

Nathalie Mallet-Poujol Research Director, CNRS. Director of Research Team for Intangible Creations and Law (ERCIM) UMR 5815, Université Montpellier I. Member of CNIL IT and Freedoms Thesis Examining Panel

Jean-Marc Manach Journalist for Owni.fr and InternetActu.net. Author of the Bug brother Blog for le Monde.fr

Meryem Marzouki Head of Research at the CNRS IT Laboratory of Paris VI (LIP6, CNRS/ Université Paris VI). President of the "Imaginons un réseau Internet solidaire" (IRIS) Association

Nicolas Nova Professor at the Université d'Art et de Design de Genève (HEAD-Genève) and the École Nationale Supérieure de Création Industrielle (ENSCI-Paris). Consultant and Researcher for "Near Future Laboratory"

Pierre Piazza Teaching Lecturer in Political Science at Université de Cergy-Pontoise (CESDIP/ LEJEP). Member of the Centre for Sociological Research on Criminal Law and Institutions (CESDIP)

Yves Poulet Rector of the Notre-Dame de la Paix University Faculties (FUNDP). Professor at the Law Faculty of FUNDP and the Université de Liège (Ulg)

Alain Rallet Director of the Laboratory for the Analysis of Industrial and Social Dynamics (ADIS) at the Université Paris Sud. Course Leader for the Master's in "Network Industries and the Digital Economy" (IREN)

Fabrice Rochelandet Economist. Professor of Communication Sciences at the Université Sorbonne Nouvelle Paris III and for the IREN Master's at Université Paris Sud. Member of the CNIL IT and Freedoms Thesis Examining Panel

Françoise Roue Economic and Financial Comptroller General. President of the "Technologies and Society" Department of the General Council for Economics, Industry, Energy and Technologies (CGEJET). President of the OECD Nanotechnologies Working Group

Antoinette Rouvroy FRS-FNRS Qualified Researcher in the Philosophy of Law. Associate of the Information, Law and Society Research Centre (CRIDS) of the Université de Namur. Member of the CNIL "Foresight Committee"

Bernard Stiegler Philosopher. Director of the Institute for Research and Innovation (IRI) at the Centre Georges-Pompidou. Professor and Director of the Research Unit "Technical Knowledge, Organisations and Systems" at Université de Technologie de Compiègne (UTC)

Cécile de Terwangne Law Faculty Professor. Research Director at the CRIDS "Freedoms and the Information Society" Unit. Notre-Dame de la Paix University Faculties (Namur, Belgium)

Henri Verdier Entrepreneur and "Big Data" Specialist. Chairman of Cap Digital Technology Cluster. Member of the Scientific Council of the Institut Mines-Télécom. Member of the CNIL "Foresight Committee"

Jean-Claude Vitran Head of the "Freedoms and ITC committee of the Human Rights League (LDH). Administrator of the Citizen Science Foundation (FSC)

Dominique Wolton Director of the CNRS Communication Sciences Institute. CNRS Research Director. Member of the CNIL IT and Freedoms Thesis Examining Panel.

Jérémie Zimmermann Spokesman and Co-founder of La Quadrature du Net. Consultant Engineer in Collaborative Technologies

The opinions collected during the interviews are personal points of view, and do not necessarily reflect the views of the organisations for whom the experts work.

PRIVACY TOWARDS 2020

Society is being radically transformed under the effect of several factors, among which are:

- the increasing influence of information and communication technologies on the organisation of society, to the point that the “always on” norm seems somehow ineluctable and irreversible;
- the development of interoperability between technological devices and their convergence with various scientific disciplines, such as brain sciences and genetics;
- the explosion of social networking services usage is increasingly contributing to an expression of the individual, and there are more and more personal data consumption around those services;
- the change in status of the mobile phone (smartphone), together with the proliferation of mobile internet uses;
- automatic personal data capture becoming the norm;
- the increasing porosity between public and private life, particularly in the professional field, due to the decoupling of work from geographical location and the moving away from compartmentalised time.

These reports present an overview of the contributions of our experts.

The first part presents some of the key transformations, already under way, which combine technological innovation, the building of new business models and the

implementation of new social practices. It then deals with social web, the monetisation of personal data, *Big Data* and the growing space occupied by algorithms in personal data processing, geolocation, biometrics, internet of things and nanotechnologies.

In light of these transformations, the second part analyses the evolution of the key concepts of "personal data", "sensitive data", the *privacy paradox*, "digital identity" and "the digital divide".

The final part suggests a number of avenues for development of the regulation of the future, refocusing our enquiry on freedoms to be preserved, by envisioning the development of new forms of both legal and para-legal regulation and offering food-for-thoughts on the recognition of new rights for the individual, compiled under a category which perhaps needs to be created: Digital Human Rights.

01



Part 0.1

FOCUS ON SOME KEY TRANSFORMATIONS

...

**IN THE CROSS-OVER BETWEEN
USAGE, TECHNOLOGY AND
ECONOMIC STRATEGY**

THE SOCIAL WEB REVOLUTION: WILL WE ALL BE "CELEBRITIES" IN THE FUTURE?	12
DATA AT THE HEART OF BUSINESS MODELS: WILL WE ALL BE DATA TRADERS IN THE FUTURE?	15
THE ALGORITHM "DICTATORSHIP": WILL WE ALL BE CALCULATED IN THE FUTURE?	18
GEOLOCATION: WHERE ARE WE HEADED ?	21
BIOMETRICS: THE NEW "OPEN SESAME"?	24
NANOTECHNOLOGIES, GENETICS, NEUROSCIENCE, "ENHANCED HUMANS": WHAT IS ENVISIONED FOR HUMANITY IN THE FUTURE?	28

THE SOCIAL WEB REVOLUTION: WILL WE ALL BE "CELEBRITIES" IN THE FUTURE?

“ The take-off of social networking services is the biggest development of the last decade. Sociologists did not foresee this "expressivist dynamic" leading to the increased desire of individuals to express themselves. Intimacy has become a personal, individualised value: it is defined in relation to a context and individual behaviours in this regard seem steadfastly divergent. Privacy is becoming a factor that determines autonomy, and free will. For some it is increasingly linked to issues of individual dignity. Each individual therefore wants to keep some room for manoeuvre. However, it would be a fundamental error to think that the notion of privacy is disappearing: in fact, the more I expose myself, the more I value my privacy; I want to be able to control the boundary between exposure and intimacy. The notion of secrecy remains very much alive. For example, it is striking to note that on Facebook most people don't discuss romantic intimacy. Also, photo posting strategies are often very sophisticated. ”

Dominique Cardon

ARE SOCIAL NETWORKING SERVICES PUBLIC SPACES?

The take-off of blogs, on-line opinion sites and social networks have played a role in developing an internet that is increasingly built around user profiles, a social internet. This social web is built around different facets of digital identity, projected differently according to the type of visibility that each platform confers upon its members. According to our experts, these spaces give rise to new questions because they are not completely public and not completely private. These zones where individuals unveil a part of their intimacy are described as , a zone of “chiaroscuro” by Dominique Cardon. Users share their social life by addressing a network made up of close friends and family, which remains difficult for other people to access. Although they number several hundred friends on social networks, in terms of personal conversations they only

communicate with around ten of these. Only this inner circle feels it has the right to take part in conversations. Others participate when discussions are more general and less intimate. In this way, they “air their identities”. Unique to social networking services is the way this border between the domain of personal, private conversation and that of totally public posting is played with. The possibility of sharing constantly threatens the compartmentalisation of certain posts and individuals dread such a “breach”.

In these grey areas, to reveal oneself takes on a new meaning. The neologism “extimate” refers to this dimension in which individuals publicly share a part of their intimacy.

TRANSPARENCY, UNVEILING AND THE MARKETING OF THE SELF

One of the consequences of the democratisation of social networks is that sharing within these spaces is not totally random. In fact, there is currently peer pressure on presence within these networks, and so, circles of “friends” are becoming increasingly broad – and may include colleagues and acquaintances – whereas these spaces were initially restricted more to close friends and family. Shared content is also more diverse, increasingly including photos and video, for example.

Within this context, the experience of self-exposure is in the process of attaining greater maturity in terms of practices, and for certain users, greater calculation along with sophisticated strategies of disclosure. For





"BIG OTHER" AND LATERAL SURVEILLANCE: ARE OTHERS BECOMING A NEW AUTHORITY?

The expansion of lateral (or mutual) surveillance is an issue that concerns a number of our experts. For Dominique Cardon, it designates all intrusive behaviours of users towards one another. Antonio Casilli explains that "to understand who is listening, you have to give out signals that will provoke reactions and comments". This is therefore the level of participation that determines the strength of the participatory surveillance of everyone by everyone: a "Big Other" world. Social acceptance of this surveillance by peers is perhaps greater in the younger generations. At any rate, this is the view of Yann Leroux, for whom this "violence" is viewed in a better light, since it is more seductive and less brutal than that which would be exercised by an authority. Each of us can watch those around us, which is a departure from the classical social model of the panopticon. If, in the case of institutional surveillance, the best regulation is certainly legal, in the case of mutual surveillance, regulation is more complex to organise, since users display their identity voluntarily. So it needs to be more social and cultural and takes the form of self-organisation. Dominique Cardon proposes transferring criticism of those who expose themselves to those who watch. Although it's difficult to take a view on the long-term consequences, Yann Leroux questions this new form of surveillance: how can one grow up without pitting oneself against an authority figure?

Pierre-Jean Benghozi, these strategies may be transparency, compartmentalizing or obfuscation. The social web allows each user to comment and to share their interests and opinions, which will have an impact upon their audience. Here there is perhaps a risk of digital digital (see "Are we headed for new digital divides?" page 40) in the management of one's disclosure, between those who are able to easily manage the different facets of their digital identities (compartmentalizing or crossing-over of personal and professional attributes) to take advantage of this (visibility, finding a job, etc.), and those on the contrary who will fall prey to exposure. According to Dominique Cardon, there is a genuine "user trajectory with its problems and set-backs which even if they are few in number, form part of the learning process". By focusing activity on the creation and staging of the public façade that the profile constitutes, social networking services incite their members to think about the marketing of their own identity. Users are constantly carrying out market research on themselves and developing "self-sculpting" skills.

... APPEAR, EXPOSE, RETREAT: BETTER CONTROL AND NEW RIGHTS

Nevertheless, privacy is not disappearing, quite to the contrary. The more individuals reveal themselves, the more valuable their private life becomes; in fact, they know how to manage the boundary between what they wish to expose and what they feel needs to remain intimate.

One essential factor, highlighted by researchers, is the preservation of context (Dominique Cardon, danah boyd, Helen Nissenbaum). More than the content itself, what individuals seek to control is the context, the meaning of a post: the place, time, "recipients" and general tone. The September 2012 controversy concerning the "FacebookBug", which led to the publication of private messages on the public part of the "wall" underlines the importance of the original context. It illustrates this spill-over effect in which posts restricted to "friends" escape from the inner circle and circulate publicly.

Confusion in the minds of users also arose from a new way chosen by the social networking service of presenting old posts that was not linked to their context. The disappearance of the original meaning of the posts made it especially difficult, several years later, to determine their genuinely private or public nature, which lent further credibility to the existence of the presumed *bug*.

For Alain Bensoussan, Facebook is a wonderful world in which one's *début* is made by "having friends" and "liking". There is no self-exposure; rather primacy is given to the paradigm of appearing. Social networking services embody the universal value of the "right to appear". They allow one to show oneself with no restrictions as to time, place or event. Dominique Cardon advocates a "right to self-exposure" and its corollary, the "right to retraction". ■



DATA AT THE HEART OF BUSINESS MODELS: WILL WE ALL BE DATA TRADERS IN THE FUTURE?

“ The personal data economy is based on a powerful leverage effect (owing to the low acquisition cost). Self-disclosure is consubstantial with the development of web 2.0 mercantile services. It is difficult for users to keep in mind the fact that a merchant is present, playing the role of intermediary. One should never forget that on Facebook, your first "friend", is Facebook: it is all-seeing and scrutinises our activities. The issue of "valuing" personal data is problematic, especially since there are no reliable indicators in this regard. What is certain, however, is that data of a personal nature does not have an absolute or intrinsic value: it depends of the context and the company concerned. Its evaluation is based on contingency (if... then...). At any rate, one finds that individuals are not very consistent in this regard: whilst in a survey they may say they are prepared to pay Eur 100 for Facebook not to sell their personal data to third parties, at the same time they are willing to hand it all over to their local store to take part in the loyalty programme and be given a few Euros worth of vouchers. So it's difficult to ascribe a financial value to personal data. The setting in place of a right to compensation in the event of exploitation of the personal data of an individual would be even more difficult, even if it were to be recognised that this right derives from a logic of legal liability and not of ownership. This economy is largely an economy of the intangible, and therefore of the invisible: the invisible must be rendered visible (particularly the commercial exploitation of data passed on without the knowledge of the individual), and transparency imposed. ”

Alain Rallet and Fabrice Rochelandet



PLATFORMS AND MAJOR DATA OPERATORS - THE NEW MASTERS OF THE UNIVERSE?

Contribution economy, attention economy: new economic models have emerged with internet 2.0. User involvement remains central and the monetisation of personal data is omnipresent, to such a degree that we frequently hear this described as "the oil of the digital economy". As Alain Rallet and Fabrice Rochelandet have pointed out "these services run on self-disclosure like a car runs on petrol".

Even though *freemium* is gaining ground, the principal model for activities on the internet consists in offering a service to users by having it paid for by advertisers. This model, which is that of platforms and operators such as Google and Facebook, leads to ambiguous relationships between platforms and users, who are not, strictly speaking, customers. All the more so since the specific features of the digital economy transform these major operators into natural monopolies of sorts (common interest in a certain standardisation, network effect). These players have acquired, albeit temporarily perhaps, a very specific position, "the spinal column, the vital personal data infrastructure". Like Daniel Kaplan, we should perhaps think about a specific status for these very large platforms, "which are operators unlike others". These digital platforms are the specific depositories of personal data: they have become its custodians and this model is based just as much upon this as it is upon the (perhaps somewhat naive) trust of users. This makes their responsibilities all the greater.



... HOW ARE OUR TRACES AND POSTS MONETISED?

This monetisation is, however, all-pervasive yet elusive, as Alain Rallet and Fabrice Rochelandet have emphasised. Therefore, is it really a good idea to view this issue from the standpoint of economics? According to Pierre-Jean Benghozi, "the pros are that it creates arbitration mechanisms, a means of regulation between supply and demand and this makes consumers aware of the fact that what they reveal has a price, a value. However, there is no proof that market mechanisms will be more efficient in the data field than they have been in the realms of finance or conventional industry". This market flaw appears very probable, given the nature of the asymmetries: "Since the compensation is not very clear about

the monetisation of this data, it is relatively easy to identify what is being purchased, but not necessarily what is being sold. Also, the unbundling of this data does not allow for genuinely clear contracts: you will always end up with a market that offers bundled payments."

IS DATA CONTROL A SOURCE OF NEW ECONOMIC ACTIVITIES?

Personal data protection currently tends to signify restrictions for companies, not business opportunities, as the experts have emphasised. Nevertheless, the future could be different and data management and protection could become a source of economic activity in the medium-term. Accordingly, "privacy could become an even more competitive and

innovative factor" says Jérémie Zimmermann, who also thinks that a genuine data protection market will exist around the issues of IT security and encryption... when these subjects become "ungeekified". The take-off of consumer *Cloud Computing* could set off this market for digital asset management.

For Dominique Boullier, rethinking the data economy from an insurance perspective would provide the best prospects of reducing a certain porosity that the current transactional, mercantile framework will only consolidate: "Insurers would be the intermediaries, who would to battle with those wishing to appropriate personal data. Data circulation is not an inherent problem, provided that individuals have a means of understanding and acting, for example with the assistance of these intermediaries. A model of regulation combined with insurance may be a virtuous mechanism."

Finally, an innovative avenue is emerging

from the idea of reciprocal data sharing between customers and companies, in accordance with the principle summarised by Daniel Kaplan: "If the company has information on the customer, the customer must have them as well" (MesInfos and MiData projects, in France and United Kingdom), whereas currently customers know less and less what companies know about them.

As Daniel Kaplan explains, "this idea is based on the concept of *Vendor Relationship Management* (VRM) created by Doc Searls, to balance out *Customer Relationship Management* (CRM)", the effects of which are paradoxically leading to an ever greater decline in loyalty-building.

For Doc Searls, the only place where the 360° turnaround is genuinely possible is customer-side and the VRM movement seeks to lay the foundations of a healthy customer relationship in the era of digital industrialisation, "requested personalisation replacing imposed personalisation", for example through the use of emerging tools designed to "tool-up" the customer and ensure their *empowerment* against companies, such as *Personal Data Stores* (MyDex, Privowny, personal.com, etc.) or intent-casting.

But how could this data be "reused" by individuals? Daniel Kaplan refers to the *quantified-self* movement: with their consumer data, the individual can think in terms of their mobility, their carbon footprint, increasing their skill set, applying eco-responsible measures to their consumption, etc.

These initiatives are seen as positive overall, even though certain experts see them as traps. Antoinette Rouvroy, for example, thinks these plans are a little naive if they disregard profiling and prediction models. For Meryem Marzouki, the danger lies in transforming the right to individual access into a kind of generalised *Open Data*, where with one simple consent, all companies can access the transaction data held by others... ■



THE ALGORITHM "DICTATORSHIP": WILL WE ALL BE CALCULATED IN THE FUTURE?

“ Everything that is happening today concerning personal data forms part of a movement of "grammatisation". This concept, invented by Sylvain Auroux in 1995, designates a process of "discretisation" i.e. a code created by individuals in society, for example the creation of the alphabet, or counting on one's fingers... Digital is a new stage of grammatisation. The first was the alphabet, the second was printing. The third stage emerged in the industrial revolution with the division of labour: the individually controlled machine-tool "grammatised" work. In a fourth stage, photography, cinema and television grammatised perception, waves and behaviours. In the current fifth stage of digital grammatisation, everything is becoming the carrier of a digital grammar, finding general expression in the internet for objects. Digital is a new social milieu, a new public space and a new stage of writing: it is used to produce data. It is also a third industrial, even hyper-industrial stage: we are industrialising, automating even the ordering of our libraries. Each grammatisation phase creates a proletarianisation process, i.e. the depriving of knowledge which is delegated to the system, that is without precedent. In this regard, Plato explained in *Phaedra* that writing could bring about atrophy of the memory and be deleterious for man by no longer providing for oral cognition, or thinking itself. Industrial grammatisation has proletarianised production (the end of craftsmanship, craft fraternities ("companions"), etc.). In the previous, analog, grammatisation sequence, it is consumption that is proletarianised, by increasing the dependency of individuals on mass-consumption. These processes are also occurring today: for example, we forget phone numbers, and doctors increasingly make computer-assisted diagnoses. ”

Bernard Stiegler



BIG DATA, SMALL DATA, CLOUD: THE NEW DATA REVOLUTION?

The concept of *Big Data* was certainly one of the subjects most frequently raised by the experts during interviews when discussing changes that could have the greatest impact over the next 10 years. Although still nebulous and difficult to encapsulate, it may be viewed as being structured around three "V"s: a significant data *volume* is certainly needed, but this threshold means nothing unless we add to this *variety* (different sources) and processing *velocity*. Technologies that offer increasing calculation powers, that are easily *scalable* since they are hosted in the *Cloud* and enable the processing of new types of data, particularly unstructured data, have encouraged the emergence of an industry worth almost Eur 700 billion in 2011 (IDATE, *Cloud and Big Data*, May 2012). Yet this "Data Deluge" is intrinsically linked to developments in usage: users are sharing an ever-increasing diversity of content (photos, videos, blog posts, micro-conversations, personal and body sensors) and the rate of acquisition of smartphones and tablets is increasing, even further encouraging the sharing of this data. For Dominique Boullier, two major new factors are emerging around this available data, giving rise to the concept of *Big Data*, beyond conventional *data-mining*. Firstly, the data processed is no longer static but dynamic and in real time: "before, we monitored a state, but now it's a high-frequency pulse", as revealed by the examples of *yield management* which change prices in real time. The other new factor is the "ease of switching scales and going from *Big* to "micro/nano" Data that represents the individual". Statisticians used to be in the habit of aggregating data and processing aggregates, but it

is now possible to "zoom" in within this data to the individual. In part, these factors indeed concern this boundary between the macro, where data is aggregated, and the potential for fixing on an individual. We create profiles and impute to individuals desires and needs that they do not express at any point and we run the risk of locking them into these behavioural avatars. This is what David Forest has emphasised, for whom the danger resides not in statistical data taken in isolation, but rather in the cross-referencing of data that appears harmless but which may result in discriminatory processing. All the more so since the algorithm that processes this data is a "black box, like the Coca-Cola recipe" so much so that it is not possible to find out the logic that underlies decision-making.

For some of our experts, the revolutionary nature of the *Big Data* phenomenon must nevertheless be relativised. This is in particular the viewpoint maintained by Daniel Kaplan, who rather sees in it the swan-song of "productivist IT, excessively centred on brute force to mobilise more data and calculating power". For him, *Big Data* is not sufficiently in the service of individuals and he would rather see a kind of *Small Data*

whereby individuals could become tooled-up so as to be able to exploit their data themselves (see "Data at the heart of business models: will we all be data traders in the future?", page 15). For Emmanuel Kessous, if *scoring* becomes widespread, the individual is deprived of the freedom to choose the company with which it wishes to conduct a transaction, whilst the freedom of choice (of customer) is offered to the company.

WILL WE ALL BE GOVERNED BY ALGORITHMS?

This is the theory of Antoinette Rouvroy, who takes a critical look at these automatic decision-making tools and particularly at the algorithms governing them. In her view, they provide an *a priori* structuring of the scope of action of individuals and bring into being a new "algorithmic governability": *Big Data* should be viewed as forming part of the "overall context of information capitalism", within which the predictive nature of data is overvalued. Within this we find a kind of supremacy of automatic decision-making even ■■■



- ■ ■ though machines cannot take everything into account, particularly causes.

We therefore go from "deduction to purely statistical induction, only retaining what can be measured, in a kind of information reductionism". In fact everything having to do with human consciousness becomes suspect, and some angles of reality elude us, since the unmeasurable no longer exists. *Big Data* encourages "digital behaviourism" that predicts behaviour and allegiances, classifying individuals on the basis of the risks and opportunities that they present, without having to compare or understand them. It is therefore an ambivalent form of "personalisation" that we are dealing with: *data-mining* and profiling permit the improvement of surveillance, and controls, individualising service and information offers, placing the citizen, the consumer, the user, "at the centre" of tools, whilst not allowing them to give voice to their intentions, desires, motivations and preferences, which are automatically inferred by digital tools. For decision-making, these technologies tend to dispense with human interpretation and evaluation, and with the public debate concerning the criteria of merit, need, desirability, level of danger, justice and equity in favour of the systematic, rather than systemic, real-time operational management of

situations. In such a context, "an ethical vision and approach for ICTs are fundamentally necessary" (Antoinette Rouvroy).

Yves Poulet also points out that the "reduction" of the individual is becoming ever greater: "The individual is currently reduced to their data and to constructs made from these data, to "profiles", and algorithmic avatars. This is a dangerous, statistical construction of individuals."

For Henri Verdier, this issue leads to a kind of "euphemisation of power" similar to that perceived by Michel Foucault in his analysis of biopolitics. Although at CNIL's creation, its priorities were data collection for illicit uses, today the new central issue is interoperability. Statistical processing enables information to be gleaned that is not intrinsically personal: "it speaks about people without being nominative". Data-based sciences will develop and we will no longer take a detour through identification or spying on the subject (such as finding out their political orientation). If power is becoming totally abstract, invisible, statistical and probabilistic, the protection of freedoms should perhaps become so too.

For Antoinette Rouvroy, *data-mining* can be cordoned off, by immunising certain sectors – those in which the theories of justice to which we collectively adhere demand that the criteria of merit, need, desirability, level of danger, etc. be considered collectively and democratically – including the management of digital footprints in those key areas having to do with the corporate responsibility of companies. These latter could accordingly take an interest in minimising their impact on the information environment in an "approach comparable to that which prevails in caring for the environment". ■



GEOLOCATION: WHERE ARE WE HEADED?

“ Geolocation is a form of data for which individual authorisation is required, and which is economically certainly very advantageous. In particular, it allows many small businesses to push their products. But people must be made aware of the importance of this data. Moreover, sociologists are currently working on the idea of geolocation and trying to understand this phenomenon from the standpoint of the user: why do people use geolocation? ”

Christine Balagué



THE BOOM IN GEOLOCATION-BASED SERVICES

Most experts interviewed highlighted the exceptional speed with which services using geolocation have been adopted: such usage has spread at an unprecedented rate even for the digital realm, essentially through the widespread acquisition of smartphones (around 75% of mobile phones sold in France in 2012). In just a couple of years, the proportion of the French more or less regularly using a service requiring geolocation has become extremely large, and, when CREDOC asked the following question "Would you like to be able to stop transmission of your location to commercial companies?", 81% of mobile users responded "yes" at the end of 2011 (see box on page 22).

This infatuation can be explained in a number of ways: first and foremost, location services are so practical that no sooner are they tried than they are adopted. And it is not for nothing that the in vogue expression for 2011 to designate the "winning" imperatives for digital business, SoLoMo (standing for Social – Local – Mobile), places "local" at the centre of

its dynamic: geolocation is seen as the holy grail for many digital business specialists, since it enables the relevance of proposals and recommendations to be increased.

What is more, it has a genuinely ludic dimension: Dominique Cardon notes, in this regard, many individuals use geolocation in parties or trendy places, (bars, etc.) ultimately to "be on stage" and also "to create talking points" around a subject, place, experience, etc. "a bit like on social networking services" (see "The social internet revolution: will we all be *under the spotlights* in the future?", page 12).

However, we should also view these technologies in a more rose-tinted light, as Alain Bensoussan has reminded us: "Geolocation is actually a day-to-day experience of the oft-vaunted merging of the "real and the digital worlds", with our minds succumbing to a merging and synchronisation of these two realities, physical and digital, the world of bytes and the world of molecules: "it confers the right to exist in these two worlds, to be present in them simultaneously, to live in both synchronous and asynchronous worlds at the same time."

So is the situation stable in this regard? Although GPS has existed for some time, we ...

WEAK SIGNAL: IN THE FUTURE, WILL WE NEED TO ACCEPT PERMANENT GEOLOCATION TO ACCESS MOBILE SERVICES? THE EXAMPLE OF "GOOGLE NOW"

One common tip for guarding against abuse of geolocation data collection is only to activate this function when using it, for example when looking for an itinerary. Will this advice still hold good in the future? Apart from the lack of clarity and simplicity in phone settings, some innovative services require permanent geolocation for optimal functioning. This is the case with the "Google now" function integrated into version 4.1 of the Google Android operating system. "Google now" claims to be a "predictive" personal assistant, the slogan of which is that it answers your questions before you even ask them. Accordingly, since it knows your daily travel habits, it sends you an alert telling you when you have to leave to arrive on time to a meeting, based on where you are currently located. So, in order to improve its accuracy, the service "needs" your location to be captured not only when required, but actually permanently (to learn your travel habits, modes of transport, etc.) So how can we be sure about the future of this permanent "location" mapping and graphs?



- shouldn't forget that these "enhanced" services are in their infancy. Nicolas Nova, feels its should be conceded that the field is still in the process of maturing around 3 types of use: proposing more targeted advertising based on one's location, knowing where one's friends are and linking a message or comment to the place where one is located. Many of these uses may rapidly overreach what is "acceptable" for these users.

WILL BEING GEO-LOCATABLE BECOME THE NEW NORM?

In a few years, Geolocation has therefore gone, according to our experts, from being an exceptional act to being something almost banal. Does this mean that it has become harmless? Nathalie Mallet-Poujol thinks that the new behaviours surrounding the emergence and now the general use of geolocation mean a greater level of acceptance of these technologies by individuals.

Being geolocated is becoming more banal, even though these users would certainly be concerned, where they to learn how easily this data can be passed on to certain players (see box opposite).

In the future, geolocation may no longer be intermittent, but permanent, as these "innovative" services will require this permanence (see box). Paul-Olivier Gibert argues that "in 3 or 4 years, it will be practically compulsory to be geolocatable to use certain services, such as taxis, etc. The problem is not so much in "instantaneous" data as in the accumulation and logging, and tracing of this data. Information that is not, in itself, very sensitive will become so when it allows cross-referencing to be carried out". Francis Jauréguiberry even sees in it a possible future stage of connection injunction: "Today, being disconnected and not immediately responding to one's mobile more and more frequently requires an explanation and ultimately a justification. Without anyone having decided this, the social norm tends towards permanent connection. It would appear that we are adopting the same path for geolocation and it is not



difficult to imagine that refusing to be geolocated will soon come to be viewed as antisocial and even suspect. Antisocial, because for example smart city services only works if each individual agrees to their individual location traces being processed for the common good. Objecting to this risks becoming synonymous with being uncivil. Suspect, because in an environment in which the norm would be universal geolocation, to refuse this would unfailingly lead to doubts and suspicion."

Geolocation, and particularly perhaps the logging in time of our locations, will then become particularly sensitive, in addition to the fact that it is very difficult to anonymise this, as has been shown by the work of Sébastien Gambs (IRISA Researcher) since it will be very easy to induce from this data the events and habits of one's life. A series of quality spatio-temporal data on a person may enable one to infer for

example places of residence and work, identity, fields of interest, habits, etc., and even any deviation from one's usual behaviour.

With permanent geolocation, it will be increasingly difficult in the future to keep this sensitive data sacrosanct: if it is entered and recorded it can be disseminated, stored "in the clouds", and passed on to third parties, which will constitute a huge challenge for the protection of privacy. However, *pervasive* geolocation, as it is beginning to be, also opens up fascinating perspectives for researchers, for example around what Nicolas Nova calls "path and passing mapping", which then enables one to think in terms of the dynamic mapping of flows of citizens. ■

BIOMETRICS: THE NEW OPEN SESAME?

“ There is a marked historical tendency concerning classification since the time of Bertillon's "anthropometrics" towards the fantasised identification of the population using scientific rationalism. The logical systems of classification are always based in practices that are designed to discriminate and categorise. Over the last ten years, a technological leap has been achieved with biometrics, RFID chips and geolocation systems: these technologies are outpacing the legal environment, so the law is increasingly being left behind. The effects of 9-11 served to accelerate the issue of police classification, favouring a mode of governance based upon fear and disquiet. Increasingly large marginal population groups have therefore been subject to tracking. Already in Bertillon's time, he wished to work on re-offenders, and this was then expanded to the insane, the itinerant and finally to all perpetrators. This goal of targeted populations which are then extended increasingly broadly always follows the same process, which tends *in fine* to make each of us a suspect. With the biometric passport and the planned French biometric identity card, each individual is made transparent in the eyes of the State. ”

Pierre Piazza

Cited by a number of experts as forming part of the major trends for the next ten years, biometrics is still relatively little used in daily life, beyond official and law enforcement uses (identity documents and police files). However, the emergence of face and voice recognition in consumer products or applications (smartphones, social networking services, etc.) perhaps signals the increased presence of biometrics in daily life. As Yann Leroux points out, the coming together of technologies and the human body is perhaps the key issue for the future.



THE MYTH OF THE BODY AS A MEASURE OF IDENTITY

The biologisation of identity is, for Pierre Piazza, a major and long-standing trend for States. The idea of the body as an identifier is not new. However, today it is reinforced with a new feature: "the body as password" (Antoinette Rouvroy). In this regard we see fingerprint payment validation coming up regularly, and attempts, largely unsuccessful for the moment, to use biometrics in access control for consumer products. According to Antoinette Rouvroy, the power of this myth resides in "the presumption that the body does not lie". For Jérémie Zimmermann, these new forms of identification, which are irrevocable and beyond the control of the individual, pose specific risks.

However, as Dominique Boullier points out, biometric data is dependent on technology and biological data doesn't ultimately convey very much about social identity. Raw biometric data has no meaning in isolation, but there is a tendency to fall prey to a false belief in biological infallibility. This belief in biological standards that offer greater guarantees is fairly typical of a scientific vision that it appears impossible to call into question. The risk then becomes that of "biologising" identities, when what is in fact created is a montage, a fiction of biological infallibility: there is a referential linking between the body and data, and so even in this case, there is a code, a referent, a chain, an institution, rather than "objective" data.

HOW SOCIALLY ACCEPTABLE IS BIOMETRICS?

Biometric data processing is seen as posing specific risks in terms of jeopardising private life and freedoms and as a consequence, in Europe, they are subject to a specific legal framework (in France, a regulatory authorisation process). Paradoxically, however, citizens appear little aware of these risks and with the exception of a few citizens' associations, display at best indifference, and at worst a certain fascination. Pierre Piazza points

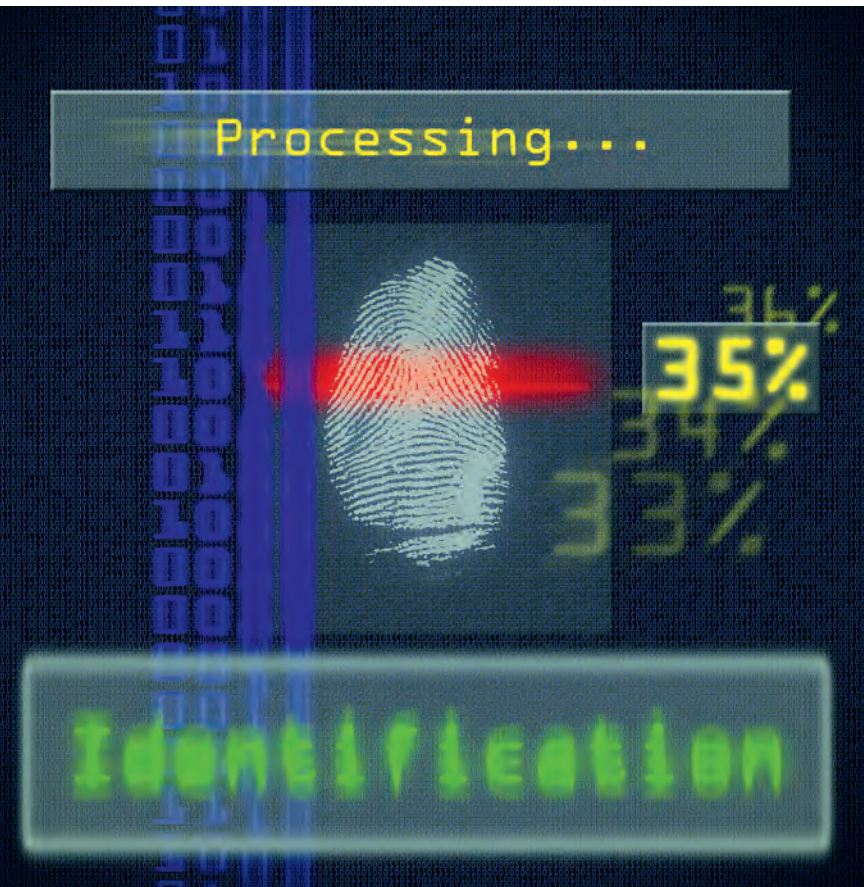


out that the population is generally highly passive and demonstrably is becoming acclimated to these technologies, namely owing to a lack of information, and because of the legitimising discourse that is put forward by industry players. Young people, for their part, appear not to show any spontaneous interest in these issues. Since few studies have been published on this point, an assessment needs to be made of the genuine degree of perception, beyond mere acceptance, of these technologies by the population.

For Christine Balagué, "understanding is the priority, first and foremost, above and beyond social acceptance". A European study by the Institute for Prospective Technological Studies in 2005 showed that these identification techniques are a source of fascination but that there is also a complete lack of awareness by individuals in regard to these issues. The fact

that biometrics is not yet very present in their daily lives no doubt explains this in large measure. Dominique Cardon sums this up by pointing out that when the average person is asked about their understanding of biometrics, they are ultimately asked more about their fascination with science-fiction movies than their daily life and their experience... Also, the fact that with biometrics – as is also the case with "contactless" technologies – the feeling of "handing over" data is lessened owing to the possibilities of automatic capture no doubt does little to arouse apprehension in the public about these techniques. For Nathalie Mallet-Poujol, biometrics – and also nanotechnologies – are increasingly acquiesced to and what is more may be increasingly used without people's awareness.

Meryem Marzouki, whilst observing that *via* video-surveillance and biometrics (for example in school canteens) social control is also being



- extended to movements and even to the body, also emphasises that it is even more astonishing that this logic of social control is accepted and even appropriated by individuals for reasons of convenience or security. Alain Bensoussan argues that there is a need to change the paradigm and "liberate biometrics", so that each individual can use personal data without authorisation for reasons of convenience or security, although with safeguards: "For example, the individual must be able to decide for themselves whether to pay with their fingerprint if that makes life easier for them."

FACIAL RECOGNITION: THE MAJOR THREAT?

Photos and images have become ubiquitous in the digital world, in particular as a result of smartphones and social networks (300 million photos are published every day on Facebook, according to the Q1 2012 results of the social networking site). "Tagging" and automatic photo identification tools are becoming widespread. As Stefana Broadbent points out, we communicate increasingly with photos and new communications genres are being created. Posting and especially "tagging" and "untagging" photos has become a major social act that is very interesting to analyse ("do I do it or not?" and for what reasons?). According to the study *Pew Internet "Privacy management on social media sites"* from 2012, 37% of US users of social networking services "untagged" one or more photos in 2011. Only 30% of people said they did this in 2009. It would be useful to have a better understanding of the behaviours and actual usage of users. Do they apply rules that are specific to the choice of photo published, their accessibility, the "tagging" of individuals? And do they do this for different types of photos (profile photos, personal photos, etc.)? What are their views about respecting the intimacy of their family and friends? In what way do they safeguard third party rights?

Another avenue for reflection: are these facial and even voice technologies reproducible (*scalable*) internet-wide? Is it conceivable that in the near future, facial recognition will be possible for all photos available on the internet?

Dominique Cardon argues that these technical developments around photography are the ultimate threat: facial recognition transforms an image into text, into code and ultimately into an identifier, whilst stripping out the context (see "Digital identity/ies: authentication for all?", page 38). And Yves Deswarte points out that since facial recognition is now very easy, photos have therefore become biometric data. It would be easy to try to extract sensitive information from them, for example, ethnicity or location.



VIDEO-SURVEILLANCE AND BEHAVIOURAL ANALYSIS

Video-surveillance is also becoming widespread and is exploring new avenues such as *Big Data* and algorithmic analysis tools to detect "suspicious" behaviour. Accordingly, a number of research projects, including DAS (New York police project) or INDECT at the European level, are being developed. Allowing an automated system to determine what is suspicious and what is not, is not without raising serious ethical questions. Pierre Piazza wonders in this regard what will become of anonymity in the public sphere in the future: "It will tend to disappear, if the individual is faced with both widespread biometrics operating "on the fly", and video-surveillance and geolocation." ■



NANOTECHNOLOGIES, GENETICS, NEUROSCIENCE, "ENHANCED HUMANS": WHAT IS ENVISIONED FOR HUMANITY IN THE FUTURE?

“ Nanotechnologies elicit a kind of fascination because “objects are invested with intelligence”. In fact, we are mistaking intelligence for interaction. Nanotechnologies risk causing a loss of autonomy of the individual over their environment. The example of GPS is revealing: the anthropomorphic conception of the computer is what leads one to say that it is more powerful than the human brain. ”

Dominique Wolton

Do the development and convergence of biotechnologies, brain sciences, nanotechnologies and artificial intelligence herald a radical transformation for humanity?

THE "WEBIFICATION" OF THE REAL WORLD

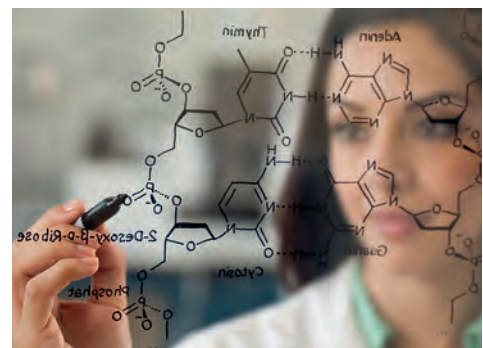
The continuing decline in the cost of RFID chips favours the emergence of an "Internet for objects". Connected objects (car, television, smart houses and "intelligent networks") will multiply. If new services emerge from such a development, they will also result in new risks for the privacy of individuals, concludes Henri Verdier. Very intimate data, passed on directly by objects based on their use will be generated and disseminated. Pierre-Jean Benghozi further notes that the activity tracks created in this manner could easily be rendered "non-anonymous", and risk disclosing the lifestyles of users, and being used in profiling. They could also be subverted for the purposes of industrial espionage (for example entry and exit of trucks in a production plant disclosed by

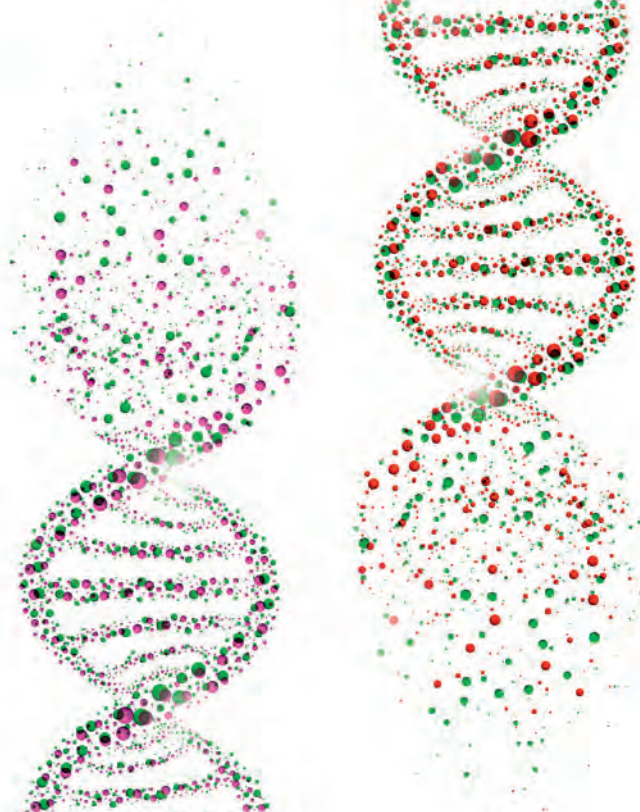
RFID chips will also be clues as to its activity). Françoise Roure feels that nanotechnologies will only jeopardise privacy if nobody exercises caution, particularly where these give rise to invisible miniaturised tools, that continuously track and watch individuals.

How can we protect ourselves from the implementation of a generalised surveillance society, against *small* and other *nano Brothers*? Jean-Marc Manach argues that the principle of caution must be applied so that nanos are neither blindly submitted to nor rejected out of hand. This was why the European Union has required that nanos be the object of a study on how they impact on freedoms. For Jean Frayssinet, it is vital that consumers are granted the right to block and deactivate RFID devices planted in the objects that they use at any time. Otherwise it will not be possible to balance the interests of the seller and the rights of the customer, which must remain an uncrossable barrier. Taking into account data protection regulation from the outset for service design, should, in this regard, be to the advantage of European companies (see "Innovations in Regulation", page 50).

GENETICS AND NEUROSCIENCE IN THE SERVICE OF PREDICTIVE SYSTEMS

Arnaud Belleil emphasises the serious threats to freedoms that could arise in the event of DNA being used in economic rationalist systems comparable to the statistical analysis used in the scoring systems of financial institutions. Between now and 2020, the field of genetic data is set to become a major "battle ground" (preventive medicine, insurance, DNA-automated analysis, etc.) for which regulatory stakeholders and citizens are





GOOGLE CREATES A "COMPUTER BRAIN"

Google recently created a "computer brain", a network of "intelligent" machines made up of 16,000 processors. The *New York Times* announced in June 2012 that the network of artificial neurones had "reinvented" the concept of the cat based on 10 million videos of cats uploaded. It was only given one piece of advice: to learn by itself. Although this network appears very much smaller than the human visual cortex, it is the first time that a programme has automatically learned how to use the data that it was provided with.

not at all prepared. For its part, neuroscience is being increasingly used, for example in the US to evaluate the responsibility and degree of threat posed by suspected perpetrators. In general, the speed with which brain science is creeping into society is striking. We now hear about neuro-economics, neuro-marketing, neuro-computing, neuro-psychoanalysis, neuro-justice, etc. All of which is, sometimes, within the ideological context of biological behavioural reductionism and defiance of all that has to do with human consciousness.

Accordingly, consumer neuroscience explores the activities of daily life, the domestic habits and the purchasing decisions of consumers to attempt to understand and nudge the mental processes that come into play within consumer decisions, and then use these alongside conventional marketing tools.

THE LURE OF THE CYBORG

Post-humanist ideologies view technology as a vehicle for disruption. They affirm that humanity must open itself up to the non-human (clones, "intelligent" objects, etc.) so that the privileged status of the human being gives way to new individuals, created by technology. In the same vein, transhumanists are fighting to improve the human condition (elimination of the ageing process, enhancement of human potential, etc.) using biotechnologies. In the US, a vast research programme, funded with several billion dollars, has been dedicated for a number of years to furthering the convergence between four technological areas, to enable

man to outperform nature: biotechnologies opening up the road to post-humanity, supported by nanotechnologies, computing technologies and cognitive science. This programme is perceived by some to be the first step towards transhumanism, which is itself seen as an intermediary step towards post-humanism.

Arnaud Belleil argues that there is a thin line between "repaired" man and "enhanced" man. Soon it will be possible to integrate technologies (electronic chips in the brain to boost memory, ocular cameras, intelligent exoskeletons, etc.) into the body. Will these devices be chosen or imposed upon us? Will they serve to increase autonomy and develop the individual, or will they be used for their surveillance? It would be good to implement safeguards without waiting to find out.

THE SPEED OF INNOVATION: IS THERE A RISK OF SOCIAL DISRUPTION?

Bernard Stiegler had previously made this point over fifteen years ago: "The speed with which contemporary innovations follow on from one another grants no respite, leading to social and psychological disorientation that is without precedent in history. With the pace of change becoming ever greater, Yves Poullet and Cécile de Terwangne fear that there is no longer pause for thought for society to become adapted, and that individuals are becoming tools and agents of the *fait accompli*, that there is no longer time to think and that technological changes are becoming more and more unpredictable. Is it still possible to respond and anticipate? Or do we now have no choice but to adjust and go along with things? Shouldn't innovation be taken out of the laboratory for debate to be held in the public domain, since what is at stake is the day-to-day life of citizens? Pierre Piazza, for his part, emphasises the fact that technological innovations are outpacing the legal environment. This means that the law is falling further and further behind. ■

02



Part 0.2

WHAT IS THE NEW LANDSCAPE FOR PERSONAL DATA, FREEDOMS AND PRIVACY?

IS EVERYTHING BECOMING PERSONALLY IDENTIFIABLE INFORMATION?	32
MORE AND MORE NEW SENSITIVE DATA?	34
PRIVACY PARADOX: THE MYTH OF ALL-PERVASIVE NEGLIGENCE?	36
DIGITAL IDENTITY/IES: AUTHENTICATION FOR ALL?	38
ARE WE HEADED FOR NEW DIGITAL DIVIDES?	40

IS EVERYTHING BECOMING PERSONALLY IDENTIFIABLE INFORMATION?

“ We no longer speak now of personal data, but of relational and transactional data. We need to stop seeing "personal data" as property and something clearly defined. Otherwise we lock up ourselves in a very narrow and closed domain. Even an identity document is transactional. This is also the case for mobile phone and bank data. All data is relational or transactional. To speak of "personal data" is to give the impression that it is a personal attribute. Transactional data is, for its part an "undertaking": for example between an individual on one hand and an institution on the other. Transactional data gives leverage to others. This is what I refer to as the "habitel": we don't possess data, we inhabit it, like our clothes, our habitat and the interior of our car. We think that we leave tracks, but this all makes up a whole, an envelope because of data interoperability. Therefore, we are "enveloped" as in a habitat. How can we direct this envelope and its porousness? Saying that we need to "protect personal data" implies "creating a bubble", which runs counter to the idea of the transaction, of the relationship. The habitel is therefore only steered inside the relationship. What must emerge is therefore the notion of mutual fragility, as with social networking services, for example. This reciprocity runs counter to the idea of the "controller of a file" thereby enabling relationships and transactions. The definitions of personal data and privacy are, for their part, unworkable fictions. ”

Dominique Boullier

"PERSONAL DATA": IMPOSSIBLE TO DEFINE

All of the interviews we conducted shared a common theme: what might appear to be the mandatory starting point and the simplest issue to think about, namely the definition of personal data, turned out to be a real conundrum. Actually, defining the concept of personal data simply and effectively seemed to many experts to be a waste of time and even a dead end. So much so that there are grounds to wonder whether the concept of "personal data" is not in fact a concept that is coming to an end.

Indeed, it seems so fluid, mobile, evolving and ultimately, subjective, that, if its use cannot



be prevented, it seems counter-productive to seek to fix it: personal data is simply increasingly subjective, relative, and contextual.

For example, for Christine Balagué, personal data that is useful from a marketing standpoint is changing. On social networking services it might be data from everyday life: what I did, what I listen to... and not just describing data (I am a man or a woman of such and such an age and living in such and such a place).

Connected objects (smart television, networked car, etc.) and internet of things raise radically new issues in this regard, which have been little debated thus far, concerning the logging and use of data that is trivial and even insignificant in and of itself, but that is likely to contribute to a very detailed profile of individuals, and to generate in respect of these latter "knowledge" (probabilistic rather than a certainty) of their personal and intimate tendencies, religious beliefs, political opinions, sexual orientation, lifestyle and indeed many other aspects of their personal and intimate life.

Alongside "conventional" personal data, we should also pay attention to other data, such as the data that Jean Frayssinet refers to as "personalised data", like the IP addresses used to create profiles, which are anonymous identities strictly speaking but which ultimately can accurately define an individual. In fact, these anonymous identities make it possible to "hone in, and raise the issue of control over assembly and profiling". Ultimately, the actual identity is of little significance in this context.

According to Christine Balagué, the next decade will be characterised by a "proliferation

IP ADDRESSES, MAC ADDRESSES, UDID: IDENTIFIED AND TRACKED BY OUR MACHINES

After a number of years, the debate on the identifiable nature of the IP address appears finally settled: for Yves Deswarte, this question no longer applies in the case of individuals: "Previously, IP addresses were dynamic, but now, IP addresses are fixed in the majority of cases. This settles the argument: the IP address is indeed an identificatory data element." Jérémie Zimmermann adopts the same position, and points out that the European Court of Justice ruled in 2011 that the IP address was a personal data element (in the case of *Scarlet Extended vs SABAM*). Today, this analysis may be extended to other machine unique identifiers such as MAC addresses (physical identifier stored in a network card) of the UDID of iPhones which are very effective tools for tracking individuals: in fact sometimes the best way of tracking an individual is to track their devices.

of retrievable, collected data which will be mapped, for example using social mapping tools and graphs". This will result in the issue of standardisation of data retrieval formats taking centre stage.

A FUTURE IN WHICH EVERYTHING IS "PERSONALLY IDENTIFIABLE INFORMATION"?

In fact, there appears to be a trend towards the increasing ease with which individuals can be re-identified within data sets that are supposed to be anonymous. Daniel Le Métayer and Claude Castelluccia feel that it is the ability to combine data that changes everything: "Can any data become identificatory when combined with "other data"? For example, the combination of a post code and a date of birth will often enable an individual to be identified. So from now on, sensitive data can be inferred from non-sensitive data. Above and beyond identification, there is the issue of profile-building, which can lead to significant discrimination across all fields of activity."

Indeed, Pierre-Jean Benghozi argues that any relatively sophisticated processing of tracks of this nature can result in data being "de-anonymised" as has been proven by experiments carried out on the purchasers of videos

on Netflix by Arvind Narayanan and Vitaly Shmatikov, and by Latanya Sweeney. In 1997, this latter, a doctoral student at MIT, was able to find the healthcare data of the State Governor from within anonymous public data using other open data sources (enabling his age, post code and gender to be determined).

This is what Paul Ohm summed up in an article published in 2010 entitled "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation": there has certainly been too much faith placed in the protective powers of anonymisation techniques. And if statistical techniques make it possible to easily de-anonymise individuals, then no longer may we limit our reflection to directly and indirectly identificatory data.

As summed up by Yves Pouillet, "from an anthropological standpoint, we no longer face an issue of sensitive data protection, but rather of the creation of constructs from trivial data". It therefore becomes much more difficult to classify the data itself, in isolation, in terms of its sensitivity (see "More and more new sensitive data?", page 34). What will happen in the future when there is a proliferation of trivial data as analysts refer to when speaking about *Big Data*? Especially when given what Antoinette Rouvroy terms "the increasing all-pervasiveness of devices", it is becoming more and more difficult to isolate a system in order to measure its risks: "We are dealing less with localised artefacts than with logistics for data sharing and circulation. Within such a context it is the trajectory and the potential meaning of "their" data that are beyond the reach of individuals."

Over the next few years, the rise of the internet of things will perhaps transform all connected objects into potential producers of personal data as a result of crossing, mixing, analysis and computation. Of course there will also be degrees: certain data will be more or less identificatory. However, the world of personal data and tracks is set to grow at least as rapidly as the world of data, i.e. exponentially. ■



MORE AND MORE NEW SENSITIVE DATA?

“ Previously, sensitive data was a component of personal data. Today, it is even possible that non-personal data will become sensitive because of *data-mining*, insofar as it is very revealing about our lifestyle [...]; digital behaviouralism may make it possible to predict behaviour and affiliations, and to classify individuals in vulnerable categories. ”

Antoinette Rouvroy

What is meant by sensitive data? With regard to European personal data protection laws, this concept defines certain categories of data deemed to pose specific risks to the protection of privacy and freedoms, and indeed the human identity, and which as a consequence have been assigned particularly highly protected status. Racial or ethnic origins, views on politics, labour relations or religion, health, sex life, penalties, convictions and national ID are therefore placed under a strict regulatory framework. As pointed out by our experts, particularly Philippe Lemoine and David Forest, the concept of sensitive data refers back fundamentally to historical concerns. Accordingly, religion and race are included in sensitive data because the law of 1978 is rooted in History, and in particular concerns the recording of French Jewish populations during the Occupation. Olivier Iteanu argues that sensitive data corresponds particularly to the values and history of the country. Here, as Dominique Desjeux points out, there are obviously major differences between countries, depending on their culture: in the US for example it is easy to speak about race or religion, which is not the case in France. And as Jean-Marc Manach has emphasised, the debate in France on ethnic statistics and the difficulties sometimes encountered by researchers in completing their studies illustrate the extent to which rigorous application can, paradoxically,

lead to an insufficient awareness of discriminatory phenomena. The issue, however, is more that of statistical security and anonymisation.

AN EVOLVING CONCEPT?

The majority of the experts interviewed shared the view that the concept of sensitive data must evolve over time and depends on the context, technologies, the use made of the data and even the individuals themselves. Should the sensitive data list be reformulated? For example, should we continue to refer to the concept of race? LICRA thinks that this term should no longer be used because it lacks any genuine scientific value. Dominique Boullier, going even further, argues that we now operate with a model that is abstract in relation to the reality of exchanges (all of our data is in fact composed of traces of our affiliations). So the system is no longer workable, even though we understand its importance within the French republican model. Isabelle de Lamberterie emphasises, however, that the specific system around sensitive data is important symbolically. With the creation of a "shared pool" there is a risk that protection will be limited. It is preferable to retain the distinction between intrinsically sensitive data and other data, even though this boundary is not always clear-cut. Yves Deswarte and Caroline Lancelot-Miltgen take the view that, in any case, this





NIR, FRENCH SOCIAL SECURITY NUMBER: NOW A NON-ISSUE?

Created under the Vichy regime, historically it was a major individual freedoms issue and was highly significant, since it specified the gender and the month, year and place of birth of the holder. It symbolised the interconnectedness of files (particularly the SAFARI project, which was the starting point behind the French data protection law in 1978). But is the French Social Security Number (NIR) still sensitive data? Curiously, although it remains a powerful symbol of the issue dealt with by the French "IT and Freedoms" Law, particularly for the CNIL, very rarely was it raised by our experts and even then only to refer to its symbolic status, which remains significant ("the NIR is the equivalent of DNA" in the words of Jean-Claude Vitran). Also, ultimately, interconnectedness and central databases are commonplace even without the NIR and tracking and identification issues are obviously no longer centred around the NIR debate.

raises an important issue regarding the classification of data itself and its sensitivity: levels of sensitivity are actually in the process of changing. For example, what is currently the status of the photo, and what will its status be in the future, particularly with facial recognition? In this regard, as Pierre Piazza points out, biometrics has indisputably changed data: there is a tendency towards the "biologisation" of identity which turns out to be "fixed", leading to traceability in time and space. For Yves Poulet, biographical data is becoming less important than "reference" data (IP, cookies, RFID, geolocation, etc.): in the future, this will be the genuinely sensitive data. Accordingly, for the Human Rights League and specifically for Jean-Claude Vitran, although the current legal ground should obviously be maintained, we also need to take into account new sensitive data.

What will be judged to be discriminatory in 10 years time? Arnaud Belleil emphasises that sensitive data may in particular be data that can be passed on from one generation to the next, like genetic and DNA data. Other highly sensitive data is found in the healthcare field, convictions and social and financial difficulties (such as payment blacklisting), custody rulings, etc. Data concerning ethnicity or sexual orientation have a degree of sensitivity that may change: within an automated *scoring* system, a postal address could be very discriminatory and may ultimately be more discriminatory than sexual orientation.

Emmanuel Kessous notes that the most sensitive data at the moment is data that may give rise to discrimination, for example healthcare data. Sexual orientation is, for its part, less

and less private, like choice of religion. This is the result of voluntary disclosure by individuals. "Currently, then, it is the potential use that may be made of data that determines its sensitivity. For example, increasingly it is the "insurance-based" healthcare system that makes medical data sensitive." So the unit of measurement and analysis has changed.

IS EVERYTHING SENSITIVE DATA?

In the opinion of Stefana Broadbent, we always think of critical information as being isolated. Whereas the information that matters, that is really revealing, arises from the accumulation of information and new algorithmic data analysis techniques.

Currently, as Antoinette Rouvroy points out, sensitive data is contained not only in personal data but also in non-personal data. Daniel le Métayer takes the view that the law will have to deal with these new issues specifically by taking into account the possibilities of cross-referencing data.

Ultimately, then, is it data that is sensitive, or the way it is processed? Nathalie Mallet-Poujol argues that although sensitive data still exists *offline*, online it is different in nature: even trivial data can become sensitive owing to the way it accumulates on the internet and the way in which it is processed: in this case, shouldn't we focus more on the concept of sensitive processing? ■

PRIVACY PARADOX: THE MYTH OF WIDESPREAD BENIGN NEGLECT ?

“ When thinking about the concept of digital identity, French digital think-tank FING found itself facing with the problem of inefficient categories and concepts surrounding the *Privacy Paradox*. Indeed, the *Sociogeeek* study, for example, actually revealed either that individuals no longer feel the need to expose themselves publicly, and in this case disclose very little, or they feel this need very strongly, and in this case strategically stage themselves via web 2.0 and social networking services. The analysis of the issues surrounding privacy in the 2.0 world cannot therefore be undertaken only from the standpoint of the concept of protection and security. In fact there are three main reasons for disclosing information on the Internet: 1/ self-awareness and self-construction, 2/ convenience, reduced complexity (optimisation, personalisation, etc.) and 3/ self-projection and self-enhancement, enabling us to reach out to others. The main reason individuals have for exposing themselves is in order to project themselves. In this context, protection is only a means to an end. It might even be said that the whole point of protecting privacy, is so that individuals can have a public life without excessive dangers. Rather than multiple identities, we should think in terms of identities with multiple facets. Suddenly, the oft-cited *Privacy Paradox* exists more in the eye of the observer than in facts and behaviours. ”

Daniel Kaplan

IS THE PRIVACY PARADOX A REALITY OR A MERE SUPPOSITION?

Making reference to the *Privacy Paradox* has, in just a few years, become *de rigueur* in any thinking on issues concerning private life. According to this axiom, individuals are growing increasingly worried in the face of a number of risks associated with personal data (identity theft, widespread surveillance, etc.) and yet, at the same time, casually disclose more and more personal data – even sensitive data – without the least assurance or control, via social networking services, in their relations with private companies, etc. There exists an apparent inconsistency, therefore, in individuals revealing themselves on the internet and via social networking services,

despite the worries that they feel about losing control over their private lives.

However, as Daniel Kaplan points out, is this ultimately a real paradox or rather an optical illusion?

The reality is that social networking services users are not as naive, according to the majority of experts interviewed. Accordingly, the most hardened among them don't always display the same identity, depending on what they want at a given time and they tend (where they know how to use the parameters) to restrict access to their profiles. Arnaud Belleil asks: "Is self-exposure a youthful mistake or an act that heralds a genuine generational divide?"

Even for those users who are less adroit in their usage of these technologies, trying to find in this paradox an explanation for the apparent irrationality of individuals is certainly the wrong approach. Although there is sometimes a disparity between actual practices and feelings or fears, this is also because the complexity of uses of the technologies is of concern to the individuals themselves, without this making them negligent or absurd, however. Ultimately, for Daniel Kaplan and a number of other experts, it would appear that this famous *Privacy Paradox* exists more in the eye of the observer – and of certain analysts – than in real facts and behaviours. Viewed as a convenient shorthand, is the *Privacy Paradox* in fact a methodological stumbling block?

IS ABSOLUTE RELATIVISM THE ONLY FUTURE SCENARIO FOR THE CONCEPT OF PRIVACY?

Why then is this myth so enduring? According to Antonio Casilli, the dominant concept of privacy is characterised by the idea that it is an absolute "inner sactum", in the direct lineage of the US concept of the "*right to be left alone*".

This viewpoint is still natural for most observers and concerns analysts: there is



something far more counter-intuitive in the concept of privacy as it is currently evolving. As Alain Bensoussan reminds us, however, we ought not to confuse secret life and privacy: the colour of my car is visible in the street, also, a pregnant woman can be seen to be pregnant, but that doesn't stop this information from being private. Yves Pouillet and Cécile de Terwangne also emphasise this change in the concept of the "personal sphere" (citing the Rotaru Ruling of the European Court of Human Rights in 2000 and the importance of the European debate on the concepts of a "personal sphere" and "expectations of privacy"). "What you do at home, show photos, play, manage your contacts, play a video game, manage your diary... is now located in the *Cloud*. It remains personal, but requires technical intermediaries. The personal sphere depends on other actors in order to function. The right is compromised for individuals *via* tools that involve third party role players. In view of this, it must either be held that as soon that there is a tool, there are third parties and data is no longer personal. The exception for private and domestic purposes is therefore no longer tenable: a totally private

sphere is preserved, but there is no longer anything in it, it's an empty shell. Or, we must broaden our concept of the personal sphere, and consequently create responsibilities for these third parties."

In reality, privacy may be viewed not as a protected inner sanctum, but as a permanent negotiation with our interlocutors. According to the work of Irwin Altman on *social penetration theory*, interpersonal relations develop over time, like an "onion": each layer opens up one after the other, within the context of each relationship between two persons. Access by others to this intimate sphere is therefore informed by a personal, individual approach. The key is therefore to be able, in the future, to marry this permanent negotiation with digital tools, for example, those of social networking services: for Antonio Casilli, the issue then becomes technical, as we must solve a complex equation in order to be able, with the assistance of unique platforms, to manage increasingly differentiated access.

Actually, the conceptual framework used to make sense of these "expressivist dynamics" — i.e. this marked tendency towards an increased desire by individuals to express themselves — has for a long time lagged behind, since, as Dominique Cardon points out, "until 2002 bloggers were seen as kids or failed journalists, even by researchers".

The range of attitudes regarding the disclosure of personal information and the many individual strategies to manage one's digital identity/ies (transparency, compartmentalisation, pseudonyms, etc.) lead to a highly nuanced interpretation of the priorities for protection and its regulation. Privacy is a contextualisation issue, and its key value resides, perhaps, as FING sums up in its work "IT, Freedoms, Identities" (Informatique, libertés, identités -FYP Editions, April 2010), in being able to choose and live out one's privacy without giving up intimacy and secrecy. ■

DIGITAL IDENTITY/IES: AUTHENTICATION FOR ALL?

“

Digital identity does not exist.

All too often, in contemporary discourse, there is confusion between identity, digital identity and the identifier. Digital identity is an aggregate, with quite blurred contours, of scattered concepts: pseudonym, identifier, log, personal and/or technical data, IP, etc. If we apply the term strictly, this concept of identity, referred to so vigorously, does not exist. We speak of surname, first name and gender, but everything else falls outside the legal sphere, or is included piecemeal via occasional stipulations. The crime of identity theft has been included in the statute book by legislators, but we still don't know exactly what the term covers! The recent French identity protection law tends to reduce identity to unvarying characteristics, like biometric data. This is too reductive for such a complex concept, and ideally we need to incorporate the concept of identity within the psychological and sociological meaning of the Civil Code. This is all a vast area of work that the CNIL could certainly take up. ”

David Forest

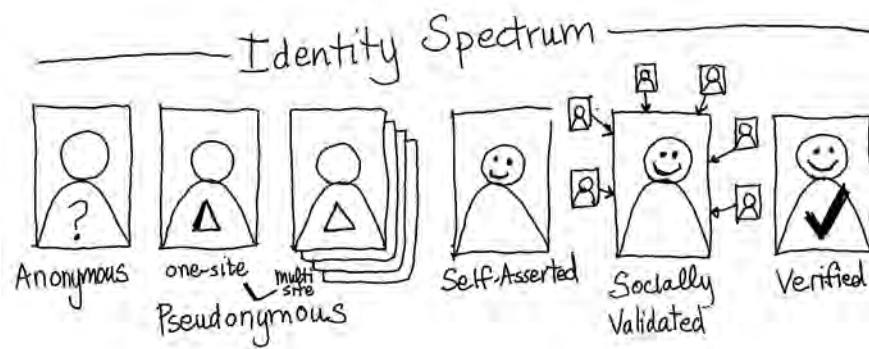


IDENTITY OR IDENTITIES?

Digital identity is a complex concept to grasp as its parameters vary so much depending on the context. One starting point might be to approach it using the attributes of identity: attributes designating individual characteristics (age, gender, address, employer, height, shoe-size, etc.) which, in combination with others, could build a profile unique to them. Accordingly, even though individuals only have one "real identity", there are multiple ways of presenting this. The transition to the online realm, which involves dematerialised separation, breaks down the projective spaces for an individual, who will then manage a number of digital identities. The digital identity of a user is necessarily split across various spheres, where each little detail may have a life of its own. The "identity spectrum" is just as varied and its different forms may range from anonymity to verified identity and everything in between, including a pseudonym or profile on a social network (see illustration opposite). This is in fact the paradox of digital life, emphasised

by Daniel Kaplan, where it is as impossible to be genuinely identified (a user cannot prove who he or she is) as it is to be completely anonymous (with IP address, cookies or browser history enabling indirect identification). This double feature is both a source of potential and of difficulties. Being able to manage the degree of correspondence between an online identity and a real identity and adapting this to the range of online worlds, be these personal, or on the contrary professional, provides genuine freedom for internet users. Alain Bensoussan, moreover, feels that digital identity encompasses a whole range of rights, among which are the right to a "multi-life", avatars and anonymity. However, managing this heteronymy is costly both in time and management for users. Identifying oneself for new services by always providing the same information encourages the development of solutions that allow authentication to be delegated, and that are more convenient and enable one to *log-in* with a single click. Where this functionality is concerned, it is *Facebook Connect* button that is the big winner, even though the various online spaces are becoming increasingly interconnected, even further limiting the possibility of being genuinely anonymous. Henri Verdier thinks it would be dangerous for Facebook to become the universal public connection, particularly for corporations, for whom the social network would turn into *Customer Relationship Management* (CRM). He advocates a public authentication system, along with Alain Bensoussan, for whom Facebook is in the process of replacing sovereign identifiers.

Pressure is also exerted on online services which, for marketing or security requirements, seek as many guarantees as possible regarding the identity of their users. Within a context in which digital identity is, for the most part, declarative, the possibility of usurpation does exist and for certain services (online banking, e-administration and online gaming for example) create a sufficiently significant trust issue for more secure forms of authentication to be sought, that enable the identity of the internet user to be certified. This debate also exists in domains that are *theoretically* less concerned with security. The French Standards Association (AFNOR) is set to propose a standard in the near



The identity spectrum: from anonymity to certified identity, by Kaliya "Identity Woman" Hamlin.
© @identitywoman

future designed to make the opinions of online consumers reliable, with identification of their authors being at the heart of the issue.

TOWARDS THE END OF ANONYMITY?

The major players such as Facebook and Google also incite their users to be present under their "real identities". Facebook is making use of *crowdsourcing* and suggesting that their users identify within their contacts those who make use of pseudonyms. Google, which at the time of launch of its social network Google+, did not authorise pseudonyms, has backtracked but at the same time incites use of the same username across all of its services to create a single, uniform identity. This trend, therefore, appears to be moving in the direction of an online identity that resembles one's real identity as closely as possible. Biometric technologies such as facial recognition pose an absolute threat for Dominique Cardon (see "Biometrics: the new open sesame?", page 24). These developments break with the traditions of the Internet which contain in its make-up the culture of "anonymity of the pioneers". The democratisation of the Internet is doing away with this learned ethos of a skilled pioneer elite and tending towards conversation and realism. The development of geolocation, consisting in placing an actual geographical position in a digital universe, is contributing to this integration (see "Geolocation: where are we headed?", page 21). Yann Leroux confirms this ever-increasing trend towards merger between the body and technology. He concludes that in the future, short of cutting off the Internet or disconnecting oneself, the right to anonymity will be increasingly contested. As proof of

this, whenever an internet user is "identified", either by their browser history, cookies or because they are connected to a service (social media, micro-conversation), it is not even certain that they will be able to conduct searches in a generic manner. This is the significance of "search personalisation" and "bubble filter" issue, where the results from a search using a search engine come to depend on the user profile. In other words, for a given search, search engines are increasingly less likely to return the same response to two different individuals. This jeopardising of the neutrality of the *search* brings a risk of fragmentation to bear by adapting content to the presumed tastes of users. For Antoinette Rouvroy, all this is not without consequences, since these filters trap users in a bubble of content which could in the long term alter their perception of the information.

Yann Leroux considers that in the future, anonymity will remain possible for those who possess the technical capacities enabling them to mask themselves using encryption tools. On this point, Jérémie Zimmermann is more optimistic and feels that individuals genuinely have an appetite for data protection and that *geek* technologies must simply be simplified and made accessible in order for these to be used by the public at large (see "Are we headed for new digital divides?", page 40). For the majority of our experts, on the horizon is the possible disappearance of heteronymity since the various facets of an identity always overlap, so that it is possible to reconstitute the profile of a user. Jean-Marc Manach goes even further, arguing that "the fifteen minutes of anonymity" will soon become a luxury. ■

ARE WE HEADED FOR NEW DIGITAL DIVIDES?

“ Thirty years ago, non-users were those who didn't have access, because of a lack of interest or financial means, to the new communications technologies. The revelation of genuine statistical inequalities regarding this access has for more than ten years focussed on the issue of a digital divide. As this was being overcome (which is still not completely the case), a much more nuanced and segmented categorisation has emerged in terms of usage inequalities, particularly between those possessing the cognitive abilities and the cultural capital to look for adequate information based on their requirements and expectations, and to process, render meaningful and hierarchise this information in accordance with a value system, and those who do not possess the means to do so or consequently to derive any genuine advantage from it. For a number of years, however, a new form of inequality has been growing around an unexpected issue: the right to disconnect. This has to do with keeping time for oneself within a context of generalised synchronisation, with the retention of one's own rhythms in a world pushing towards acceleration, with the desire not to be constantly bothered in an intrusive telecommunications environment and with the wish to have space to think where immediacy and urgency force one to react all too frequently out of impulse. The ideal that is sought after is not to be cut off from telecommunications flows but to be able to manage them, i.e. to use them without becoming a slave to them. This ideal is very unequally distributed between those who are at liberty to disconnect without this being of any consequence and those who are required to remain connected, due to professional or relationship obligations, or face penalties. ”

Francis Jauréguiberry



NON-CONNECTED, DISCONNECTED, NON-DIGITALISED

The *Unplugged* study by Havas Media from September 2012 identified two categories of disconnected populations: victims of the digital divide and the "voluntarily disconnected". According to CREDOC, 25% of French citizens do not have access to the Internet.

This figure rises to 44% for households with an income below 1,500 € per month. After a number of years of regular decline, the number of "involuntarily disconnected" has remained

relatively stable since 2010. Undoubtedly, the rapid penetration of smartphones has enabled households to have a connection without a computer. But their relatively high cost prevents them from being seen as a solution to the digital divide. In the meantime, the lack of connection increasingly limits access to resources and to services. It tends to become an obstacle to social integration and even to employment. Involuntary disconnection is becoming a new source of inequality, which is concentrated among the poorest of the population. Currently, a third of the French are "out of the loop" since they are non-digitalised, which Christine Balagué refers to as "the third-net".

Voluntary disconnection is subject to different reasons, either to do with protest or with quality of life. Christine Balagué speaks of them as the "indignant ones or the "Occupy" movement of the digital world, who reject info-obesity" and favour *slow* in the digital world as well.

For Alain Bensoussan, the digital divide will only increase. Reducing this is one of the major roles of the CNIL, because it creates a digital hazard: "The more the divide increases, the more certain populations will be at risk, particularly children. Those who are not currently on Facebook are behind the curve."

DISCONNECTED = SUSPECT ?

Exhortations to make use of digital technology are very forceful, both professionally and within society, as Josiane Jouët points out. This is particularly the case for individuals who are required to build up a personal network (professional contacts, friends, etc.). Francis Jauréguiberry feels that irreversible developments are already underway. "In an enhanced environment, it will become increasingly difficult to move around without the assistance of mobile technologies. Inside a "smart city" environment, deciding to get rid of these technologies would result not only in making life rather difficult for oneself, but also in running the risk of being considered a pariah. "This is how anonymity within society is in the process of disappearing, although it's a core concept of modernity. Pierre Piazza emphasises resistance by individuals (for example fingerprint burning) or groups (Human Rights League, various organisations, etc.) which certainly exists. But their audience within society is difficult to evaluate. The general population seems very passive and has been seen to become

accustomed to digital technologies. "One might therefore imagine that those individuals seeking to escape from these technologies will by their very nature be viewed as suspects. "It is therefore especially worrying that the imperative for connection, for a digital presence should become a new social norm: "If you're not on Facebook or you don't *tweet*" affirms Jean Frayssinet, "you almost become suspect, you are socially excluded."

Some experts argue that the fact of not having a presence on social networking services could be seen by some employers as a negative trait. For the moment the imperative of an online presence is limited merely to certain jobs (for example, certain journalists have to *tweet*). What will happen if absence from the internet were to become a handicap in the recruitment process or a new source of discrimination? We are not far from what Antoinette Rouvroy terms, after the US lawyer Margaret Jane Radin, the "domino effect" or the "slippery slope": "The mere procedural safeguarding of the right to an IT privacy and the requirement for consent do not appear sufficient to protect one against discriminatory practices in a context in which disparities in terms of power or means do not place the parties to a contract on an equal footing. An act of renunciation of a right such as the right to privacy is not merely a *self-regarding act*: it also has an impact on society since voluntary disclosure by certain individuals of certain information within a competitive context such as that of employment or insurance forces everybody else to disclose the same type of information themselves or risk being at a competitive disadvantage, or having their refusal to disclose interpreted — by an employer or insurer — as a sign of impaired risk."

CODE OR BE CODED? THE RISK OF A DIVIDE BETWEEN GEEKS AND THE GENERAL PUBLIC

But another digital divide could rapidly arise around knowing how to use monitoring and protection tools. This is summed up by Henri Verdier who refers to the risk of seeing a "new aristocracy emerge", a *geek* elite who know how to ensure their anonymity, or their peace of mind, when required, through the use of sophisticated tools such as encryption, complex parameters, anonymisation tools, virtual private networks, etc.), whereas the rest of the population would have only

one alternative: either not to use these tools or to agree to be read like an open book. As was emphasised in Lawrence Lessig's famous "*code is law*", a number of political choices are now dissimulated within questions of an apparently technical nature: as Henri Verdier observes, will the choice of tomorrow not be "programme or be programmed"?

Jérémie Zimmermann points out that, in 1995, the general roll-out of encrypted e-mail was anticipated... but didn't occur. Indeed, the willingness and desire of users was hindered by the lack of accessibility or awareness of such technologies and by the fact that they always require time. In the interests of convenience and simplicity, such aspects tend to be neglected, since they provide limited gratification to those who are not interested in the technological side of things. This is why he thinks it is vital not to make the same mistake again and not to cater only for *geeks* and other technology enthusiasts. In order to prevent a new digital divide, there must be a digital learning and education stage.

This issue of "positive" usage instruction is fundamental in the opinion of Jean-Marc Manach, who points out that "the younger generations protect themselves better than previous generations on the internet. Parents and teachers are therefore those who need to be educated to stop them from being afraid". For him, the "real problem with the internet lies with those who aren't on it and wish to lay down the law."

REDUCING THE DIVIDE BETWEEN THE "IT AND FREEDOMS" AND THE FREE SOFTWARE WORLDS

There is still one more divide, which should be easier to overcome! Philippe Lemoine points out that the "IT and Freedoms" world and the free or open software worlds have not, paradoxically, ever had any close ties in France. Until now, free and open software advocates viewed advocates of data protection as adversaries, allied with the holders of intellectual property rights, or part of the "old world". Actually, these two sides certainly have a great deal to exchange, particularly regarding the creation of new formats for regulation. It is inevitable that they will come together, for example over their concerns about the spread of *Cloud Computing*. ■

0.3



Part 0.3

PROTECTING, INNOVATING AND REGULATING IN THE FUTURE

DEFENCE OF PRIVACY OR FREEDOMS?	44
PROTECT WHOM, PROTECT WHAT AND HOW?	46
INNOVATIONS IN REGULATION	50
RETHINKING DIGITAL LAW ?	54

DEFENDING PRIVACY OR FREEDOMS?

“ The historical context of the *Informatique et Libertés Act* (IT and Freedoms law) has become, for some, totally anachronistic. Although it may be true that the debate in 1978 had been highly retrospective in nature, at a time when the ordeals suffered during the WW2 Occupation era were still remembered, there is nothing to suggest that discrimination on the basis of community, race or religion is merely a thing of the past. So the question remains: in the event of a crisis, how might these technologies be made harmless? For example, were the risks taken in India in biometric record-taking of the entire population really assessed? History is not without its tragedies in this regard. However, the concepts surrounding the issue of "ICT and public freedoms" have never appeared more relevant, as revealed by events in the Arab world: freedom in the use of information and communications technologies have become a major component of individual and public freedoms. Placing the emphasis on the effects of ICT on freedoms would enable the full complexity and the paradoxical nature of these technologies to be better grasped. ”

Philippe Lemoine



the proliferation of information disseminated over the internet, the development of self-exposure on social networking services and the ambiguous nature of the privacy policies of some of these. This new position has not caused the previous one, which pitted individual freedom against public safety, to disappear, but it appears more conciliatory, because the parties involved are more numerous and more diffuse and because they embody contradictions, being at the same time favourable to transparency and to the protection of privacy.

THE PARADOXES OF PRIORITISATION OF PRIVACY

This concept is currently actively evolving and as such is increasingly difficult to pin down. No longer does the conventional definition apply that pits it against the public domain, since, as Josiane Jouët points out, the current time is marked by great porousness between public and privacy. Even though technology is not the only explanatory factor, the all-encompassing nature of the digital realm makes it different from previous media: no aspect of social life has escaped its process of innovation which is interacting with societal innovations.

Antoinette Rouvroy takes the view that "a number of trends are in operation, which challenge the concept of the private sphere: the increasingly irreversible interactions with technological tools; and the growing interoperability of these tools with each other; the ever-greater blurring of the distinction between social and intimate time and between work and leisure time which is linked to the significance of networked working. Work is being detached from location, and work time is becoming decompartmentalised. With the permanent immersion that this implies, the concept of the private sphere becomes problematic."

A RECENT SHIFT IN THE LINE OF QUESTIONING

Judging by prevailing general debate, the central, perhaps even the sole, objective of personal data protection is the safeguarding of privacy. The culturally dominant concept in the US of *privacy* is in fact increasingly becoming an area for thoughts and debate in Europe. Olivier Iteanu points out that originally, the IT and Freedoms law was aimed at State records and files (law enforcement, courts, tax, etc.) and records concerning vulnerable persons. First and foremost, the debate pitted individual and public freedoms against public security, which were presented as being antagonistic concepts. For its part, privacy was covered by article 9 of the Civil Code, in particular... and invoked mainly by *celebrities*.

Arnaud Belleil argues that a new position, somewhere between the transparency of privacy and the preservation of secrecy, has emerged in recent years, with new data storage possibilities,

THE THREE DIMENSIONS OF PRIVACY IDENTIFIED BY FABRICE ROCHELANDET

1/ Secrecy, which implies the ability to control the use and sharing of one's data. Associated with this is the right to be forgotten.

2/ Tranquillity, the "right to be left alone", not to be bothered by unsolicited disturbances, which presupposes control over the accessibility of one's private sphere.

3/ Individual autonomy, the sovereignty of each individual over their person and what they wish to retain control over without this necessarily being kept secret. Privacy therefore amounts to the "the human desire for independence from the control of others". In France, the right to freedom of self-determination (*libre disposition de soi*) is traditionally associated with freedom of expression and physical integrity.

The great turning point came with the arrival of web 2.0, explains Alain Rallet. Being centred around content generated directly by internet users and around self-disclosure, web 2.0 involves individuals much more intimately.

Moreover, Emmanuel Kessous points out that in modern societies, under the influence of political liberalism, the social contract made provision for control by the State in exchange for respect of the private domain. Today, however, data capture and collection technologies challenge this equilibrium. Sometimes the result of this is that information from the private domain is made publicly visible. This is a trend that the sociologist Richard Sennett had already anticipated in the 1970s in this book *The Fall of Public Man*, in which he decried the "tyrannies of intimacy". Emmanuel Kessous adds that the concept of privacy is hardly in keeping, in any case, with the current quest for visibility on social networks and the emergence of tools to facilitate self-disclosure and the publicisation of the public sphere. This is a world in which one is supposed to attract attention, "create a buzz", be visible. This shift already existed in the 1970s, when advertising and marketing began to justify the use of private data to create consumer goods, regardless of the risk of manipulating individuals. Nathalie Mallet-Poujol argues that we should nevertheless fight the discourse that challenges the concept of a privacy, even where this means protecting the individual against themselves.

MONOPOLISATION OF THE DEBATE BY CERTAIN ISSUES

Major technological changes have taken place over the last few years: tracking by social networking services, biometrics, geolocation, nanotechnologies, etc. At the same time, Nathalie Mallet-Poujol observes that our understanding of the risks has not improved, quite to the contrary. On one hand these changes highlight a general trend towards the mobility of individuals and data. On the other hand they deflect the attention of lawyers and orthodox opinion from conventional Information and Freedoms issues, having to do with State records and the most vulnerable populations (foreigners, detainees, etc.).

Jean-Claude Vitran and Maryse Artiguelong even go so far as to say that: "The presentation of social networking services as being more

dangerous than government initiatives in the area of datamining has resulted in partial demobilisation of the population and in the disappearance of all debate on the dangers of interconnectedness. This is why there has only been mobilisation by the public around data bases for children and healthcare issues."

RISKS ASSOCIATED WITH THE PROGRESSIVE CONCEALMENT OF FREEDOMS ISSUES

There is concern that some vital aspects of data protection (defence of the rights of the individual and the collective against discrimination) are being eroded, at a time when some barriers are at risk of disappearing. Pierre Piazza argues that "the effects of September 11 accelerated the issue of police databasing, promoting fear and worry-based governance. With the biometric passport and the planned French biometric identity card, each individual becomes transparent in the eyes of the State". Meryem Marzouki confirms that a major sea-change has occurred in the area of protection of the citizen against the State since September 11, 2001. Accordingly, whereas the 1997 directive on personal data protection in the telecommunications sector limited the keeping of personal records, this logic has undergone a reversal since this date. The bolstering of societal control over individuals, particularly as regards the most vulnerable population groups, now appears beyond debate. Some individuals appear even to want to participate in this, to better monitor their family (for example, parents video-monitoring their nannies). The desire to detect any and all forms of danger at a very early stage (delinquent tendencies, at-risk clients, etc.), before these take concrete form, has become the norm at the risk of over-estimating the predictive properties of the data processed. Video-monitoring, geolocation, and biometrics mean that social control can be extended to an individual's movements and even to their body. ■



PROTECTING WHO, PROTECTING WHAT AND HOW?

“ We are moving towards a reductive view of data protection. Priority is given to an Anglo-Saxon "individualising" approach centred around data. By focusing on the protection of data, we lose sight of why data protection exists, which is vital, namely the issues of privacy and freedoms. For example, on airport scanners, we have isolated the data protection subject, created a precise scale of which data is likely to be processed, which users are legitimate and how long the data will be stored for and we have lost sight of the more vital issues of human dignity, freedom of movement or whether or not to disclose one's health status... The vision of *privacy* as the origin or the precondition of all freedoms is a European vision. This vision is little shared by the rest of the world, where *privacy* is understood as "confidentiality" rather than "privacy". The European vision must be preserved. The place of the individual in society is at stake. ”

Yves Poulet

PROTECTION OF PERSONAL DATA OR OF THE INDIVIDUAL?

When the French IT and Freedoms Law is evoked or indeed the whole body of European law in this regard, the current convention is to speak in terms of personal data protection, a shorthand that is certainly convenient but nevertheless highly reductive. As Paul-Olivier Gibert points out, however, the priority is not the data itself, but the sovereignty of the individual over their personal data.

Indeed, the objective pursued and articulated in the very titles of such legislation is to protect individuals with regard to the processing of personal data. There is certainly an intention, therefore, to safeguard the right of each individual to protect their personal data (a right enshrined in the European Charter of Fundamental Rights) but beyond this, as article 1 of the IT and Freedoms Law sets out, the intention is also, at a deeper level, to ensure that IT is at the service of each citizen and does not jeopardise human identity, or Human Rights,

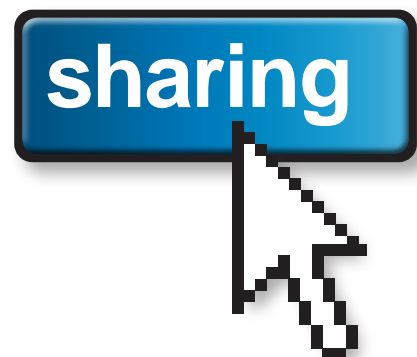
or the right to privacy, or individual or public freedoms.

But is this vision of the isolated individual pitted "against" the omnipotence of IT still applicable today? Should we continue to seek to protect individuals despite their wishes?

Opinions are divided. Many experts argue that this view, which a number of them term "paternalistic" (as Emmanuel Kessous points out, it is difficult to define autonomy on an *a priori* and identical basis for all individuals. Indeed, in IT, this latter is highly dependent upon the technical skills of individuals), is in fact outdated and must at least be modified or supplemented in the light of new social practices.

Olivier Iteanu points out firstly that in 1978, the issue of privacy was never really addressed: "The law dealt above all with records and public freedoms issues. In the last 10 years, the major change has been that public exposure concerns everybody. Also, broadcasting is accessible to all and is no longer restricted to traditional media. What is more, broadcasting operators vary in terms of their treatment by the courts in France, which is problematic."

This observation is seconded by Paul-Olivier Gibert: "The IT and Freedoms law does not address all issues. As it happens, it does address very well what an entity that is a custodian of personal data can do, within the context of execution of a contract or of a prerogative of a public authority, for example ... However, certain issues are far less well addressed, for example those dealing with the self-production and publication of personal data by the individual themselves. In this case it is an individual decision (it is not Facebook that decides to make the disclosure): this issue did not exist in 1978. Today, therefore, we must both protect individuals and adopt an approach that allows them to protect their personal data from the technical





and legal standpoints and to control its usage."

And as Alain Bensoussan points out, "first there must be recognition of rights, through data ownership, and then subsequently, protection must be provided on an exceptional basis, if necessary. Priority should be given to the individual being able to determine the degree of sensitivity to be accorded to their data and to their publication and use, and protection values should be introduced. But freedom to decide must be the fundamental principle, and protection the exception".

Antoinette Rouvroy is more circumspect: "Although the individualistic approach of data protection legislation (which presupposes that individuals are free, rational and autonomous, and as it happens, does little to protect values such as privacy *per se*) is perhaps workable, sometimes it serves as a clearing house. Perhaps sometimes it would be better not to have a protection system, as is the case in the United States, where the right to the protection of privacy is not enshrined in a specific law, which in fact makes possible a permanent debate on the *legitimate interest of privacy*. For this expert, "regulation is certainly useful, but has perverse effects: it distorts the debate, and even does away with public debate. It gives an impression of protection that is a little excessive. It protects formal rights but raises the issue of the effectiveness of those rights: reality does not spontaneously comply with legislation".

In the same vein, Caroline Lancelot-Mitgen points out that although individuals generally know that regulation exists and are aware of the CNIL, they are wholly unaware of the content of the law or the missions of the Commission: "In fact, they have a false sense of being protected by law and fail to take precautions. CNIL's

decisions, alerts and campaigns may therefore prove counterproductive: they give the impression that regulation limits any harmful consequences, that an authority is dealing with these issues and that individuals for their part need not do anything. In the United States, individuals are more militant since they are not under this illusion of institutional protection."

Jean Frayssinet makes exactly the same point: "Since 1978, there hasn't really been any mobilisation, even by consumer organisations, in comparison with the United States, Scandinavia or Germany. French society is passive and poorly organised; it doesn't take any action or it "makes noise" about incidental issues. The guarantor is the State. People have rights, but don't use them". Françoise Roure is even concerned that between now and 2020, "demands will no longer be made by society with regard to the protection of privacy because people will no longer be intellectually capable of doing so, and will no longer understand the meaning of such protection".

Philippe Lemoine warns us: "We are living in a period of increased *momentum* in our fascination with technology, and even one of genuine technological determinism. In fact, faced with a society that has in some ways lost its bearings, these technologies seem to be a source of stability and positive progress. As Edgar Morin points out, enthusiasm is not normal in society: it is a major sociological marker. Technologies appear to be taking up places left vacant by other concepts to enable individuals to feel in control of their world. The reality is that such a phase of fascination can only be temporary, lasting only as long as it is synchronous with the illusion of control."

Yves Pouillet seconds this viewpoint. There ■■■

- ■ ■ is no longer any time for thinking, because it can't keep up with technological change which is, in any case, "unpredictable". Given this context, the concept of consent is hardly valid any more: for example, the question of whether or not to be on Facebook is unfortunately no longer asked.

SHOULD NEW RED LINES BE DRAWN?

Along with other experts, Daniel Kaplan takes the view that the approach of protection alone is certainly not sufficient, since too much "protection" might cut off the individual, "insulating" them from society. The protection approach only works if linked to positive, proactive action. For him, however, "red lines will always be needed: there exists an asymmetry of power and information and there remain questions that it shouldn't be possible to ask. Regulation must be retained, therefore, and action should focus on three key areas: protection (necessary but insufficient), the empowerment of individuals (through the provision of tools, for example) and education and information".

Antoinette Rouvroy also supports the idea that certain types of usage should be regulated, for example *data-mining* and profiling – an opinion that is also shared by David Forest, Daniel Le Métayer and Claude Castelluccia: "What is needed in particular is more thorough analysis on the use of profiling for differentiated treatment of individuals. This issue extends beyond legal and technical concerns; it should be treated as a political and social issue: in which cases may the practice of differentiated treatment of individuals be considered socially acceptable and in which cases, on the other hand, should it be deemed to be discriminatory and unacceptable."

"Preventing discrimination on medical grounds, for employment, for access to credit, on the basis of court history, etc. must remain one of the most sensitive roles of the CNIL. *On the other hand*, it should be possible to regulate spam prevention under consumer law or using technical applications". Arnaud Belleil feels that

the CNIL therefore needs to prioritise.

Meryem Marzouki, for her part, takes the view that the time has come "to make biology and biometrics "sacrosanct", since this is the most sensitive data, just as the body, blood and organs are sacrosanct. Why would we have the right to sell our most intimate data more easily than our blood? Moreover, invoking "ownership rights" over personal data is by no means to be taken lightly: is personal data protection, then, not a fundamental right, but merely an ownership right? In any case, its protection as a fundamental right is already far from being secure. What if it were to become no more than an individual property protection issue? Since self-regulation is largely a trap, it is market regulation that would be liable to be imposed. Protective legislation must therefore be retained, just as strong consumer protection legislation exists, and we must move towards a global legal framework, which remains the only effective framework. The big question is how effective existing rights are. How can one really give "informed" and "free" consent, for example, in the domain of *Cloud Computing*? Also, the right of access may well be guaranteed, but it is not exercised: it is a formal right. New ways must be found of applying it".

Isabelle de Lamberterie asks: "Shouldn't users of new social media be treated as irresponsible "consumers" who require protection? Certain acts are impulsive, and in certain respects, citizens should be protected against their individual behaviour. In this respect, the principles of the IT and Freedoms architecture should be consolidated. Some fictions are to be retained (namely consent, as a "symbolic" obligation as Christine Balagué puts it) even where in practical terms, they are difficult to implement.

Dominique Wolton observes that ultimately the IT and Freedoms architecture is robust, and fit for purpose, since it is based on values and principles that don't need to be adapted to each technology. It is the new technologies that need to adapt to legislation which must retain a universal dimension, with such limited adaptations as may be made necessary by the rapid development of technology.

Dominique Boullier argues that "IT and

INVOLVING THE JUDGE

The emergence of court-based jurisprudence must be encouraged in the field of IT and Freedoms. This was the opinion of many of the experts interviewed. Some of their suggestions are cited below.

"We need a couple of significant legal rulings that would serve as references. With the exception of a few rare disputes in the area of employment law, there is in fact no, or very little, jurisprudence of any really determining significance on social networking services (and in particular on the issue of photo publication), although this would be highly desirable: clear legal signs need to be given, which is not currently the case." - **Dominique Cardon**

"Since the CNIL cases almost never come before the Public Prosecutor's department, they do not become jurisprudence!" - **Jean-Marc Manach**

"There is in actual fact very little significant jurisprudence or major rulings to which to refer in the field of IT and Freedoms. In the criminal field, Public Prosecutors fail to find any evidence of public order offences, even though IT and Freedoms law is indeed a criminal law. In the civil field, there is equally a paucity of jurisprudence; there is a lack of "case law". Lawyers mostly provide advice or carry out pre-litigation proceedings. The CNIL has handed down more rulings and effected more sanctions than criminal judges since 1978, but these are not discussed very much." - **Olivier Iteanu**

"In France there have been a lack of legal rulings to direct thinking." - **Jean Frayssinet**

"The CNIL has found itself with a paradoxical obligation: it was supposed to communicate and be kept informed, but it ended up occupying the entire discursive arena to the extent that it became the dominant voice, obscuring argument, and also undermining the role of the judges. Indeed, it is seen more as a judge than as a regulator. But the judge presiding over, and guaranteeing, freedoms, is and must remain the court judge by application of the separation of powers: this is the natural judge for personal data. It is not the role of the CNIL to be a "stand-in judge". Only the threat of legal action in court is clearly understood by Anglo-Saxon companies, particularly the internet giants. It's a cultural thing: they seek to avoid it at all costs." - **David Forest**

Freedoms legislation is necessary, but the current version is obsolete. Personal data and privacy are legal fictions that don't work (see "Is everything becoming personal identifiable information?", page 32) since they are contrary to actual practices. Data – which can now be classed as transactional or relational, and no longer as personal– will circulate regardless. We will have to confront some serious security issues... and, unfortunately, it is only then that we will act... Regulation is vital but will be "toothless" if it rests solely on this doctrinaire perspective of personal data and identity".

Pierre Piazza feels that "the IT and Freedoms architecture is doubly ill-suited, first and foremost because its principles can't be applied, particularly as regards certain State authorities. How are sanctions to be applied against public bodies, when the State itself does not apply the regulations? And secondly, owing to the internationalisation of data exchange and in particular transatlantic exchanges (*PNR*, the *Swift* case, etc.)".

David Forest formulates a contrasting viewpoint: for him, the French data protection law is sound, since it contains concepts with variable, adjustable content and general principles. But it has "lain fallow". It has been referenced a lot, but the enforcement aspect of it, for example, has been little applied. So it is difficult to conduct an assessment of its enforcement. Companies are only just starting to take it into consideration. This has to do with the role of the CNIL, which perhaps occupies too great a place within the law.

The majority of experts feel that our regulatory framework ought therefore to be adapted, and Alain Bensoussan even thinks that we should seek to create a digital fundamental rights law (see "Rethinking digital law", page 54). ■



INNOVATING IN REGULATION

“ So, what will the regulations of the future be? The various types of regulation: through technology, procedures and institutions, are all necessary. Ideally, therefore, regulation in the future will be a combination of these different facets, in addition to the vigilance of each individual and personal best practice. On the technical side of things, prudence is essential: the examples of DRM and French online tax declarations credentials certainly reveal that the speed of innovation rapidly does away with any purely technical form of regulation. It is easier to adapt these "soft" regulatory mechanisms. In practical terms, law and administrative regulation certainly have their limitations but no more so than the implementation of a technology (for example a chip). Companies, for their part, appear prepared to invest in labelling processes, in the light of the success of ISO standards, for example. Such processes would guarantee the integrity and quality of data management. But if there are few controls, and penalties are light, few companies will invest in labels or *Privacy Impact Assessments*. The difficulty also lies in knowing what one is labelling: is it a company, a specific data processing process or a product? It is not just isolate technological elements that must be labelled, but rather everything that depends on data. It has to take account of the whole information collection and processing process and subsequent onward sale. A system that combined a standard of this type and awareness raising among consumers regarding their personal data could encourage companies to certify their transparency and their excellence in the field of data processing. ”

Pierre-Jean Benghozi

NEW CONFLICT ZONES TO INVESTIGATE: THE INFORMATION WAR, SKIRMISHES, AND SOCIETAL CONTROL

As a theater of operations, regulation has become increasingly complex and fragmented, according to the majority of the experts interviewed. No longer will a regulatory framework be able to operate effectively on the basis of regulation alone: technologies, standards and labels, trusted third-parties and markets will need to be increasingly mobilised and supplemented by personal vigilance behaviours. The regulation of the future will need to be organised around mixed processes encompassing law, economics, new tools, the dissemination of technologies, communications and digital literacy. It will need to be accompanied

by the training of individuals through digital education that cannot just be— or even largely be — education about risks and harm: priority must be given to teaching on usage and best practice, which is more effective than teaching about risks (which doesn't work, or no longer works, as Jean-Marc Manach, among others, has pointed out). In fact, as Alain Rallet and Fabrice Rochelandet affirm, in such a scenario, regulation will have to go through a kind of "information war" between the key stakeholders of the digital economy: a series of "skirmishes" in the field of public opinion may in effect redraw the battle lines in one direction or another, to allow for the new norm to emerge.

Arnaud Belleil argues that beyond an Anglo-Saxon vision (which itself changes more than one might think) of a system in which self-regulation and the market are *in theory* sufficient, regulation must be moved forward into the future, in the words of Pierre Tabatoni, with a "protection system" encompassing law, economics, activism and technologies in which all these components are mutually reinforcing. Neither should we rule out a scenario in which new players play a not inconsiderable role in the regulation of the future. Accordingly, Emmanuel Kessous argues that the setting in place of a system of third-party certifiers to guarantee transparency in relation to consumers (what kind of data, how long will it be stored, etc.) needs to be explored. This route, involving the emergence of intermediaries, insurers (Dominique Boullier thinks that insurers could facilitate the internalisation of risks within transaction costs, as is the case for bank and credit cards) and auditors, is certainly to be explored if "bringing into compliance" is to become a core mission of data protection authorities, since as Daniel Le Métayer and Claude Castelluccia note, if the CNIL cannot audit everything itself, it must be able to distribute and supervise controls. Some also think that provided that it possesses the necessary autonomy and skills, a Data Protection Officer (or in French a CIL, "Correspondant Informatique et Libertés") could in the future become a true "compliance manager" for its organisation. According to Yves Poullet and Cécile de Terwangne, what matters *ultimately* is that society must take a stand, and there are a number of ways of organising this "societal control", for example through *class action* mechanisms or through the development of debate at the European level and through the taking of clear-cut positions by legislators. Arnaud Belleil



also thinks that in this field, France needs a "collective action" type mechanism like class actions.

PUTTING THE INDIVIDUAL BACK INTO THE CENTRE OF REGULATION

Regulatory action must strive to reduce information and power asymmetries between economic or institutional stakeholders and individuals by better informing these latter and through the creation of tools and services centred on the individual. Empowerment of individuals, assisting and enabling them to protect what they wish to protect and to exercise their rights, is a major priority for regulation in the future. However, it would be an error to think that individuals can manage the burden of regulation alone: although they must play a role in it and although regulatory action must work towards their empowerment, the liability cannot be on the individual alone. Alain Rallet and Fabrice Rochelandet take the view that it would be inefficient and unfair for individuals to have to assume the burden of regulation, even though this would encourage a necessary learning process. The cost of regulation must therefore also fall upon operators, although care must be taken not to curtail innovation.

They point out that, as the work of behaviouralist economists has shown, placing too much weight on individual choices can be counterproductive. Accordingly, Alessandro Acquisti has shown that individuals reveal much more data when they think that they are in control of it, whether this control is substantive or not, in what he refers to as the "illusion of control".

Cases of security breaches also reveal that as long as there is no visible damage, individuals quickly appear to forget about this. Jérémie Zimmermann furthermore emphasises the

need to increase both the financial and the image "costs", of such breaches to make companies take responsibility for these, whereas currently they tend to silence or minimise these breaches, for example by creating within legislation the obligation to provide precise, individualised and targeted notifications on all "leaked" data.

For some, all this suggests that *Privacy Enhancement Technologies (PETs)* will be vital to tool-up individuals in the future. However, the assessments of the experts interviewed regarding their value diverge widely. Daniel Le Métayer and Claude Castelluccia, argue that, generally speaking, *PETs* are already available. The following, in particular, may be cited: anonymisation tools, management tools (that enable each individual to fine-tune how they express their personal data protection wishes), data noise or perturbation tools (where absolute exactitude is not required) and encryption tools (the importance of which are emphasised by Yves Deswarte and Jérémie Zimmermann).

For these experts, however, there is no guarantee that a mature *PET* market will develop, since nobody is investing heavily in this, as there appears to be a very low "willingness to pay" amongst users for the moment. For other experts, the idea of a reconciliation through technology is illusory and even dangerous: "Surveillance and privacy are opposites and must remain in conflict. *PETs* are necessary and useful, but must not dispense with democratic debate on collective priorities, which cannot be reduced to technical solutions increasing the individual control of users over "their" data" (Antoinette Rouvroy). For Caroline Lancelot-Miltgen, another approach for returning power to consumers is to encourage "user control" mechanisms through systems that would rate and rank companies. A great deal of protest has already been seen regarding sales practices emerging on Facebook or Twitter: we should not underestimate the fact that, sometimes, as Daniel Le Métayer points out, "users vote with their mouse".

Finally, one solution for the future is perhaps first and foremost, as Dominique Cardon recommends, to transfer our criticism from "those who expose themselves to those who watch" and thereby ensure that legislation primarily concerns those who watch rather than those who expose themselves (see "The social internet revolution: will we all be *under the spotlights* in the future?", page 12).



“ In the future, *a priori* regulation will become increasingly difficult to instate. Therefore, *a posteriori* regulation becomes more important: those using data need to provide reports. In fact, just as in society one is not permitted to spy on the inhabitants of a house through their windows, it should not be possible to make inferences about them with total impunity: data use must leave traces that may be verified by third parties. And in order to enable this verification, the "interface design" component is important, as shown, for example by the Google dashboard which allows users to see at a glance what information they are sharing with the service, although this would not be sufficient. In any accountability system, we need to draw upon the principle of sincerity, on "accounts" being provided and on the possibility of verification by an auditor. The personal data protection authority could endeavour to set out recommendations and standards to provide a framework for the procedures of Data Controllers which would in turn facilitate audits. The Data Controller would then know what they were required to store and be able to present in the event of an audit in order to prove that they had acted loyally. This type of process would "flesh out" the accountability principle for personal data, thereby enabling a kind of "CNIL" quality standard to take shape. At the same time, we would need to ask how we could "tool-up" individuals, even if the tools were not sufficient in and of themselves. For example, one might imagine software agents who would be the "representatives" of the individual on a given machine, for the management of their personal data, which would be tantamount to a sophisticated form of parametrisation. ”

Daniel Le Métayer and Claude Castelluccia

... WHAT ROLE FOR DATA PROTECTION AUTHORITIES IN THE FUTURE?

Evidence of the insufficiency of a single national framework is such that all parties are calling for increased cooperation between authorities at the international level, and particularly at the European level. Such exchanges need to take place both on the definition of standards and in concert with major public and private stakeholders. Yves Pouillet and Cécile de Terwangne argue that the authorities are the "watchdogs of privacy", with an increasing tendency to become "jurisdictions" since they are given oversight missions and because of their make-up: they are therefore becoming conventional legal bodies. These protection commissions are not debating platforms, therefore, but rather are locked into their protection mission. In the future these will need to be positioned upstream, at the level of thinking and debate, forecasting analysis and research agendas, as suggested by Françoise Roure and Antoinette Rouvroy, for example. Moreover, Meryem Marzouki thinks that *privacy by design* must absolutely be encouraged in research contracts. Genuine efforts must in the long-term be made jointly

by the authorities and the research community. It is in fact vital, argues Pierre-Jean Benghozi, to combine a policy of protection and a policy of openness and facilitation at the European level, so as to promote innovation under acceptable conditions. According to Yves Deswarte, the CNIL could incentivise research financing organisations, or even help to launch pilot projects for privacy protection tools. Companies, for their part, will not take the plunge unless they are forced to. The CNIL has a showcasing role to play for these protection technologies and could even promote their development.

The authorities must also expand their horizons by working with new partners. Jérémie Zimmermann, Jean-Marc Manach, Yves Deswarte and Philippe Lemoine are thinking in terms of the — complex, proteiform world — of free software (see "Are we headed for new digital divides?", page 40).

In the long-term, the CNIL must, argues Bernard Stiegler, be reformulated to promote and even lead the necessary emergence of a digital civil society. Indeed, to use the analogy of "digital pharmacology" made by Bernard Stiegler, the CNIL must act as a physician: it must diagnose and "prescribe". But it must also enable the patient to manage their own digital "health status" themselves, as any doctor would. Philippe Lemoine points out that originally, the CNIL was conceived of as a "social conscience for the Nation" but never really espoused this role: "The issue that the CNIL is grappling with is one of the weightiest and most significant of all, far more so than that of intellectual property rights over information assets. It must pursue external growth by welcoming new areas of debate on digital freedoms and rights, such as for example those associated with data openness."

After all, as Yann Leroux points out, whatever happens, the role of an authority is always important, if only because the fact that it exists means that one can complain about...

"API-SATION" OF ONE'S DATA MANAGEMENT?

R egulatory innovation must take the form of tools and new forms of action for personal data.

In Arnaud Belleil's opinion, the principles of data protection remain solid. However, they need to be made more operational by finding ways to adapt them to current usage. The real priority is therefore to enable a rebalancing to take place of information asymmetries that exist between organisations and individuals. No

longer should we enforce the right of individuals over their data using a defensive logic, or as a recourse in the event of a dispute. Rather, new modes of interaction must be instated between stakeholders. At the centre of these lies the principle of transparent and symmetrical access to the data held. Dominique Cardon backs this necessary renewal in which the user could decide which data to store and which data to delete in the CRM of the operator, for example, using a simple interface configured as a dashboard showing one's personal data.

This is what Daniel Kaplan seeks to promote through the Fing "Mes Infos" (My Info) project designed to restore balance to relations between individuals and organisations (see "Data at the heart of business models: will we all be data traders in the future?", page 15). Starting from the principle that new "open" data is personal data, an *Open Data* logic needs to be extended to such data (which would not be accessible to the public, but only to the user that it concerns). Technically, one way of facilitating direct and transparent access is through the use of APIs — (Application Programming Interfaces) — which can be envisioned as "sockets" that organisations could make available to their users, to which these latter would be able to "plug into" in order to access and modify their data. Using an API would thereby make data more directly accessible for users at the same time as it would deliver this in a standardised format that could be read by other machines. In this respect, advocating the opening of an API would not only involve a technical architecture but a more general design making it easier to reuse data by delivering it in a format that would promote its interoperability.

TOWARDS NEW RESPONSIBILITIES FOR HOSTING PROVIDERS?

According to Paul-Olivier Gibert, a specific statute needs to be enshrined in law for hosting providers who would not be responsible for data processing. Accordingly, they would not be able to retain user rights for themselves over the data and their sole obligation would then be platform provision. This hosting statute would then be accompanied by the implementation of a certificate for the organisation concerning its *privacy policy*. Hosting providers could, for example, be obliged to provide at any moment, and on an ongoing basis, the tools required for personal data protection (such as *privacy by design*, accounts configured to the strict minimum, by default). Also,

a central tenet of Paul-Olivier Gibert's argument is the labelling of hosting providers, an issue which has been abundantly commented upon by our experts.

WHAT ABOUT LABELS?

A label-based certification mechanism appears to be an interesting path for a number of our experts. Emmanuel Kessous, takes the view that a labels market is liable to develop insofar as these constitute a trust signal that communicates the positive reputation of a company. The label therefore represents an economic opportunity, particularly for companies wishing to distinguish themselves.

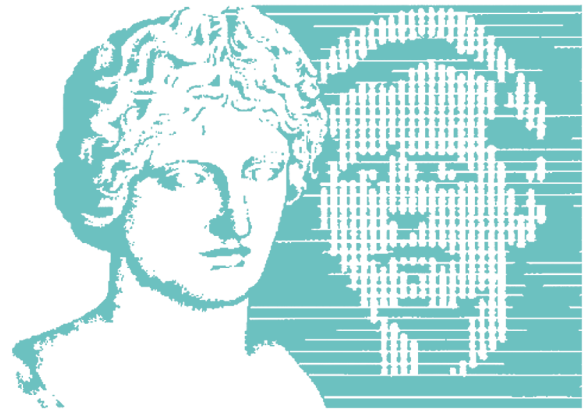
Labels could also prove dangerous in as much as they could be manipulated by companies. Philippe Lemoine argues that these are liable to adopt tactical behaviours in order to be labelled. For this reason, Nathalie Mallet-Poujol feels that their credibility would be highly dependent upon audits and associated fines. She adds that a label-based certification system would need to be open to challenge. Yves Deswarte, for his part, takes the view that labelling would be an incentivising device but that it would require major user-side awareness-raising efforts. Although the idea is compelling, governance could prove complicated and presuppose prior creation of benchmarks with CNIL approval.

Finally, Emmanuel Kessous suggests a middle-path with the creation of a minimum legal foundation to be supplemented by a number of possible levels of labelling. Companies could in this way be provided with incentives to move towards labelling to attest to their transparency and excellence in the field of data processing. ■

RETHINKING DIGITAL LAW?

“ Regarding Human Rights, not all fundamental rights have the same status, with some being more important than others. The right to the respecting of human dignity is the only right that cannot be derogated from. Dignity must be respected as an absolute value. The issue of personal data could take into account this implicit hierarchy among fundamental rights. Since the European Human Rights Convention is a more complete "catalogue" when talking about Human Rights, a link must be established between IT and Freedoms and those rights and freedoms enumerated in the European Convention. ”

Mireille Delmas-Marty



THE RIGHT TO BE FORGOTTEN: A POLITICAL UTOPIA OR A GENUINE PRIORITY?

The right to be forgotten is poorly understood, explains Arnaud Belleil: we are not talking about the right to erase systematically all of one's data, or the right to falsify archives and therefore the past, as undertaken by the main protagonist of the novel *1984*. For Isabelle de Lamberterie, the right to be forgotten must be thought about in a society in which the right to preserve and the duty to remember exists.

In enabling an individual to have certain data erased more easily, this right in fact centres around enabling them not to see their life hampered by reminders about their past. The place of court rulings on the internet, in respect of which the principle of anonymisation has been questioned by the CNIL, is a good example of this. Dominique Cardon goes even further, and considers that "the right to lie is an essential right": technologies shouldn't prevent people from hiding certain information. Olivier Iteanu argues that the right to be forgotten should be organised temporally, perhaps linked to the the right to information, with provision made for the right to anonymisation of online items after a certain period of time. Other proposals have

also been put forward: Yves Deswarte contemplates the allocation of an erasure date each time data is ceded. Dominique Cardon mentions the implementation of an actual system of evaporation or erosion of personal data in chat rooms and social media. He emphasises the usefulness of reminding network users what they said the year before, for example, so as to enable them to sort, store or erase their data (see box). Emmanuel Kessous, for his part, suggests implementing an expiration date into social networking services, a date which would take into account the type of content and the development of tools designed to monitor the scheduled deletion (even though there is no way of technically guaranteeing compliance with the rule in the case of data copying). He also cites the possibility of cache memories being systematically deleted every 18 months, although he would prefer less radical solutions. In the same vein, Daniel Le Métayer and Claude Casteluccia feel that even though the right to be forgotten "is in reality impossible to impose internet-wide", this does not mean that the development of tools that facilitate the systematic erasure of data and verification subsequently that these mechanisms had not been sidestepped may not be envisaged (*accountability* issue referred to above).

Pierre-Jean Benghozi approaches the issue from another standpoint, that of the right to remember, which is just as important on the internet as the right to be forgotten: can it be said that content still belongs to the person that placed it on line? He takes the example of the online file saving service *Dropbox* which stipulates in its general terms of use that it has legal ownership of any file stored by the programme. The result is that nothing prevents these service operators from keeping records

LEARNING TO MANAGE OUR DIGITAL MEMORY

Clive Thompson, a feature writer for Wired magazine, explains that in the long term, users will need to act as true archivists. Until now, individuals didn't have very many records of their private life. But with online publication spaces, storage methods are being transformed. External memory capabilities are increasing and by becoming digital are becoming different in nature. Soon we will need to manage years of emails, enormous piles of memories and therefore to be able to decide what to through away. Thinking like an archivist would involve learning not to register and to eliminate traces that were deemed not to be relevant. This writer explains that individuals have a natural tendency to be hard with their former selves. An archival perspective would also enable them to be reconciled with themselves.

of such files. What recourse does the internet user have against this service when it finds out that data concerning them has been erased? The issue of the right to archive personal data seems even more problematic than the right to be forgotten, particularly since the development of *Cloud Computing*. The issue of definition of a data portability right is even more crucial.

DATA PORTABILITY IS A POWERFUL REQUIREMENT. WHAT TOOLS ARE NEEDED?

The setting in place of a right to data portability should serve as a vital lever for its protection. Jérémie Zimmermann links this to the issue of the right of access, which needs to be reformulated so as to incorporate an interoperability requirement, recourse to open formats and the right to select the format through which to pass on one's data. Consequently, data portability should lead, where possible at the European level, to a real "obligation to pass on personal data concerning you". Pierre-Jean Benghozi takes up the issue of interoperability standards and emphasises the need to be able to create safeguards for one's personal data.

For Daniel Le Métayer, the absence of portability is one of the reasons for the imbalance between the user and services such as Facebook, since the individual forfeits the possibility of exercising their rights, specifically the right to renounce an online service without restrictions. In his book *The Intention Economy*, Doc Searls sums up this asymmetry, explaining that the general terms of use for these services are generally "velcro" on the part of the service and "glue" on the part of the user. The portability right is already present in consumer law (portability of mobile phone number, of banking services). A number of our experts have emphasised that the merchandising of personal data gives rise to new regulatory issues that combine protection of privacy and consumer law.

Daniel Kaplan does not trust in the good will of economic stakeholders to do away with the entry barriers that protect their markets. In his view, portability will need to be imposed upon them, which will then lead to them advocating the development of acentric social networking services (such as *Diaspora*).

NEW SUBJECTIVE RIGHTS TO ADDRESS NEW CHALLENGES

A great many of the experts interviewed feel that it is vital for individuals to be granted a more active role in the regulatory tools applied to them. In order to deal with the new risks of jeopardisation of individual rights and freedoms, Antoinette Rouvroy proposes recognition of new rights, as an extension of access rights:

- the right "to an unpolluted mental environment", already promoted by a number of anti-advertising groups;
- the right to define oneself personally, since identity is not a phenomenon but a process and one's identity is constructed by becoming aware of who one is (see the works of the American philosopher Judith Butler);
- the right to reject profiling by automated processes that judge and classify individuals without their knowledge;
- the right to access the reasons why a given profile has been allocated to you.

Alongside this, Paul-Olivier Gibert would like individuals to have at their disposal personal data protection tools, both legal and technical, in order to protect their data themselves and retain a level of control over its circulation (through encryption, etc.) and deletion.

THE RIGHT OF OWNERSHIP OVER ONE'S DATA: A BAD IDEA IN DISGUISE?

A laïen Bensoussan notes that certain social networking services maintain ambiguity by requiring their users to sign a licensing contract. However, granting individuals ownership rights over their personal data is not without its dangers. Meryem Marzouki argues that it is tantamount to saying that personal data protection is no longer a fundamental right or an individual right. It would not be facilitated, far from it, rather. A "right of ownership" in fact implies a "right to be stripped of ownership", adds Nathalie Mallet-Poujol, whereas an individual right is inalienable whilst permitting, where applicable, financial compensation, controlled use, etc.... and the removal of this right where it is in the public interest.

This risk of adding to social division is emphasised by Francis Jauréguiberry: "The poorest might be tempted to sell their data, whereas ...



■ ■ ■ the data of the rich would be more easily preserved." Christine Balagué wonders what the extent of the right granted would be: "There is a chance that the right of ownership of individuals might only concern their raw data, and not data scored or enriched by a company." Alain Rallet and Fabrice Rochelandet point out that, in any event, the value ascribed to "ownership" would of necessity be variable, since it would be dependent upon its anticipated use. It would therefore be impossible to ascribe a value to data outside of a specific form of processing or context. Pierre-Jean Benghozi adds that the exclusive right granted to individuals over their data would run up against the same limits as copyright, with the same difficulties to ensure enforcement, locate the heirs, etc. Therefore, it would be largely illusory.

REINFORCING CERTAIN ASPECTS OF CURRENT REGULATION

Nathalie Mallet-Poujol emphasises the utility that there would be in granting full scope to the concept of end use and purpose. Although designed as the cornerstone of the current legal system, it has always been under-utilised. Instances of violation of this are numerous. All too often, out of convenience, jurisprudence merely invokes the principle of proportionality and makes no mention of whether the end use of data processing is either legitimate or appropriate. In her opinion, however, undertaking such an examination would mean less room for subjective assessments. Antoinette Rouvroy proposes a tightening of the usage criteria of, on one hand, group profiles, statistical concepts which can be the source of

significant discrimination, and, on the other hand, *data-mining*. Finally, Claude Castelluccia and Daniel Le Métayer would like to see in place a principle whereby all data use must leave verifiable traces (the *accountability* principle).

IN SUPPORT OF DIGITAL HUMAN RIGHTS

“ Digital dignity would mean fundamental, natural, universal rights and principles, enabling one to live in the virtual world: the right to anonymity, since one rarely needs to use one's real identity on the internet; the right to change one's life; the right to manage multiple identities, create avatars, specialised virtual doubles made up of accretions of personal data that are truncated transfers of our identity; the right to use a non-signifying identifier, with no reference to one's real identity, and a virtual address; the right to start again from scratch, a variation of the right to be forgotten; the right to transparency, meaning "you won't do anything to me that I don't understand". ”

Alain Bensoussan

Faced with private companies that behave like quasi-States and manage individual identities seeking to profile these so as better to be able to sell them, a system of Human Rights for cyberspace needs to be promoted. Such an approach could make use of various initiatives: "A Declaration of the Independence of Cyberspace", published on February 8 1996 in Davos by John Perry Barlow, co-founder of *The Electronic Frontier Foundation*, and a public figure for the libertarian internet "pioneer"; The "Internet Rights and Principles" Charter, issued by an international working group formed in 2005 and primarily composed of jurists, which has been in discussions since that time, and the "Cyberspace Bill of Rights" drafted by the journalist and blogger Jeff Jarvis, centred around digital rights. In France, a Bill is in project, and, generally speaking, the idea has the support of the Human Rights League, in the name of which Maryse Artiguelong and Jean-Claude Vitran feel that the right to personal data protection must be "constitutionalised" and that there must be movement towards a digital *habeas corpus*". ■

HOW IS THE LAW TO BE INTERPRETED IN THE FACE OF CHANGES IN TECHNOLOGY AND SOCIAL PRACTICES?

Mireille Delmas-Marty, you use the idea of "fluid law" with regard to data protection. Aren't you concerned that this concept will undermine the principles of clarity and the binding character of legal rules?

Mireille Delmas-Marty: Not at all! "Fluid law" doesn't mean obscurity or ineffectiveness but rather flexibility. Subject to certain conditions, it enables us to legislate for the one and the many. It provides a means of having recourse both to common principles and to differing techniques and practices, that are tailored to local situations. This allows for margins of appreciation and adaptation to be managed within a shared legal framework. The concept of the "national margin of appreciation", used by the European Court of Human Rights is an illustration of this. It is intended to bring together the universality of the rights and freedoms of the Universal Declaration of Human Rights and Cultural Diversity, the value of which for mankind was declared in 2005 by UNESCO within the Convention on the Protection and Promotion of the Diversity of Cultural Expressions.

Should there be an effective framework for the margins of appreciation that are thereby granted to the various stakeholders?

Of course, a single body must oversee the compatibility with the shared principles of the various solutions chosen in positive law, so as to prevent any risk of arbitrariness. This is because fluidity means not a lack of thoroughness but rather even more thoroughness and transparency. It must be combined with indicators for the acceptable variability margin, so that it is understandable and predictable. The compatibility thresholds must also be made explicit. Organised in this way, law can be

evolving and innovative, since there is no longer any need incessantly to change the reference standard.

Isn't this approach particularly well suited to Europe?

Yes, this is true. A margin of appreciation is in any case implicitly recognised each time a European text refers to national public policy. However, at the current time, this technique is used increasingly rarely, since the authorities prefer to make the law uniform, even where this means forgetting the specific provisions of national legislation. Accordingly, in the field of data protection, there are plans to move from a Directive to a Regulation. Actually, threats to personal data are often associated with national economic interests or specific cultural characteristics. So much so that standardisation of the legal systems of European countries doesn't seem to me to be a very realistic objective.

How is the idea of fluid law an idea for the future, particularly as regards data protection?

The application of a "fluid logic" has become vital at the European or global level.

It is particularly necessary in democratic States in the field of privacy and more generally speaking for any freedom that is combined with restrictions. In the field of personal data protection, there was a turning point with the September 11 2001 attacks and the reaction that followed. There were some drifts in enforcement, allowed by quick technological innovations. The ambivalence of new technologies is now striking: they enable both a consolidation of democracy and widespread surveillance by each individual over the collective. How can

we keep the positive aspects whilst at the same time preventing such misuse? We can respond to technological innovations with legal innovations, but it is very difficult to design evolving law. The legal responses often lag behind the technologies. But, whether we are talking about bioethics or data protection there is a constant need to adapt the legal standard to take into account the acceleration in innovation. Independent administrative authorities are undoubtedly best equipped to carry out this role, by using both *soft law* and *hard law* and by not hesitating to implement a logic of gradation.

Should we conclude from this that there is no longer a place for "hard law"?

Certainly not. Hard law is indispensable, but it can be vague (imprecise) in the circumstances set out above, whereas soft law, (whether non-binding and/or sanctionless) can be precise. This soft law has a specific function: to express undertakings entered into at the ethical level. Generally speaking, soft law is not deserving of our unequivocal praise. The more one leaves margins for interpretation to the judge, the more they will need to be provided with precise performance indicators and weighting scales for those indicators. These could, for example, be in the form of CNIL recommendations serving as reference behavioural standards.

APPENDIX INTERVIEW FORM

Privacy, freedoms and personal data towards 2020. What are CNIL's priorities for protection and regulation? Positions, perceptions and expectations of stakeholders.

TECHNOLOGICAL, ECONOMIC AND SOCIETAL DEVELOPMENTS IMPACTING UPON THE PROTECTION OF PRIVACY, FREEDOMS AND PERSONAL DATA

Developments and impacts of the past and present

■ What are some of the major changes that have taken place over the last ten years, that seemed to you to have an impact on the protection of privacy, freedoms and personal data?

With regard specifically to individual behaviours in terms of privacy and freedoms, self-exposure and in the light of demands for personal data:

■ In your opinion, are the social changes we are seeing concerning the relationship between individuals and their personal data and protection of their privacy essentially associated with technical developments or are these transformations intrinsic to contemporary society?

■ Finally, do you consider that the IT and Freedoms architecture (designed in 1978 and amended in 2004) has been sufficiently "adapted" in the light of these past and present transformations? For which reasons?

Developments and impacts in the next 10 years

■ What do you think will be the emerging or new risks (threats), that will be liable to prey upon privacy and freedoms? Will new "red lines" need to be drawn?

■ Will there be new data that is "sensitive" and other data that isn't so sensitive?

■ How do you think the new boundaries between the public and private spheres will be redrawn?

■ How might the contours of the concept of privacy change?

WHAT PROTECTIONS AND WHAT REGULATIONS IN THE FUTURE?

■ Over the next 10 years, what will be the key transformations (those that you are already aware of and those that you perceive to be possible or probable, or even those that you fear) that you think will be of major importance for

the protection of privacy, freedoms and personal data?

■ What form of regulation do you envisage for the future: self-regulation by individuals, legal regulation, market regulation, regulation through technology, co-regulation?

■ Do you think that the rights enshrined by data protection laws (the right to access and correction of one's personal data, the right to information, the right to object and the right to prior consent) will be effective when faced with future transformations? Will new rights need to be defined (e.g. the right of ownership of one's personal data)?

■ Do you think that "regulation by technology", by IT tools enabling individuals to protect their data ("privacy protection technologies" *PETs*, "obfuscation" or "shading" techniques, etc.) should be encouraged?, how could a market for *PETs* be promoted?

■ Could certification or labelling play a role in this? By whom?

■ What roles will companies be required to play in the future in the regulation of privacy? And of personal data? Should new obligations be introduced in their regard? Should other stakeholders be brought into regulation? (telecom carriers, technologies designers, etc.). What forms of regulation by the market could emerge?

■ What will be the involvement of civil society in the future in terms of protection of privacy and freedoms (extent, forms, new players)?

YOUR ASSESSMENT OF CHANGES (PERCEIVED, DESIRED) IN THE ROLE OF AUTHORITIES, SUCH AS THE CNIL IN THE FUTURE

Particularly as regards the following areas:

■ Powers, modes of intervention and evaluation of their efficiency

■ Relations with stakeholders, players

■ Statute, composition and financial means

■ Roles at the European and international levels

■ Should we move towards a European data protection authority?



**Commission Nationale de
l'Informatique et des Libertés**
Direction des Études, de
l'Innovation et de la Prospective

8, rue Vivienne - CS 30223
75083 Paris CEDEX 02
tel.: +33 (0)1 53 73 22 22
fax: +33 (0)1 53 73 22 00
deip@cnil.fr

www.cnil.fr

